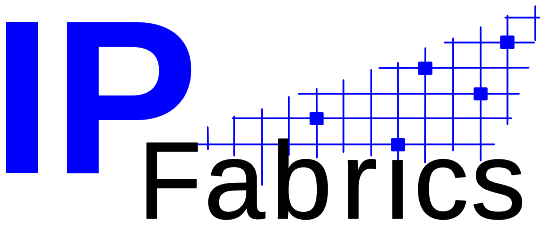


DeepSweep™

User's Manual

Release 1.44
October 2007

Copyright © IP Fabrics, Inc. 2007

IP Fabrics Corporate Headquarters
14964 NW Greenbrier Parkway
Beaverton, OR 97006
Telephone (main line): 503 444-2400
Telephone (FAX line): 503 444-2401
Website: http://www.ipfabrics.com

Information in this document is furnished in connection with IP Fabrics products. No license, express or implied, to any intellectual property rights is granted by this document. This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license.

Copyright © 2007, IP Fabrics, Inc. All rights reserved.

DeepSweep™, Packet Processing Language™, PPL™ and PPL-VM™ are owned and copyrighted by IP Fabrics, Inc.
Microsoft®, Windows® and Windows® XP are registered trademarks of Microsoft Corporation.
Linux® is a registered trademark of Linus Torvalds.
Red Hat® is a registered trademark of Red Hat, Inc.
RedBoot™ is a trademark of Red Hat, Inc.
MontaVista® is a registered trademark of MontaVista Software Inc.
Intel®, XScale® and Pentium® are registered trademarks of Intel Corporation.
Java™ is a trademark Sun Microsystems, Inc.

Table of Contents

1 Introduction....5
2 DeepSweep™ Overview....6
3 DeepSweep™-1 Installation....9
3.1 Hardware Setup....9
3.2 DeepSweep™ Power-up and initial configuration....11
3.3 DeepSweep™ Use with a Network Tap....11
3.4 DeepSweep™ Use with a Single Traffic Stream....12
3.5 Firewall settings - "iptables"....12
3.6 Time Synchronization – "NTP"....12
4 Using DeepSweep™....14
4.1 General DeepSweep™ Configuration Page Layout....14
4.2 User Accounts and Account Management....15
4.3 Operational Overview....17
4.3.1 Administration Pages....17
4.3.2 Run Pages....20
4.3.3 Surveillance Assembly Pages....21
4.3.4 Surveillance Modules....30
4.3.5 Surveillance Module Actions....32
4.3.6 Databases....34
4.4 Evidentiary Records....35
4.4.1 Contents....35
4.4.2 Enabling Evidentiary Records....35
4.4.3 Location of Evidentiary Records....35
5 Creating User Defined Programs for DeepSweep™....37
5.1 Building the User Program....37
5.2 Available SA Services....37
5.3 User Program Configure, Load, and Run....37
6 Creating Classify Databases....39
7 Creating Patterns Databases....44
8 Accounts and Ports Information....46
Appendix A –'iptables'reference firewall file....47
Appendix B –'ntp.conf'reference file....48

 Copyright © IP Fabrics, Inc. 2007

Table of Figures

Figure 1. DeepSweep-1 front view 9
Figure 2. DeepSweep-1 rear view 9
Figure 3. Mgt-port to switch connections 10
Figure 4. Top view with cover removed. 10
Figure 5. Side view with card cage elevated 11
Figure 6. DeepSweep Page Layout 14
Figure 7. Login Page 15
Figure 8. Admin Account Management page 16
Figure 9.User Account Management page 17
Figure 10. Administration Tab, System Interface Page 18
Figure 11. Administration Tab, World View page 19
Figure 12. Run Page 21
Figure 13. Make Surveillance Assembly Main Page (Known SAs) 22
Figure 14. Make SA Tab, Connections Page 24
Figure 15. Two PIXL Surveillance Assembly Connections Configuration 25
Figure 16. Complex Connections configuration page 26
Figure 17. Make SA Tab, SM Chains Page 27
Figure 18. Make SA Tab, SM Actions Page 28
Figure 19. Surveillance Assembly Options Page 29
Figure 20. Make Surveillance Module (SM) Page 31
Figure 21. DeepSweep Monitor Page 33
Figure 22. Real-Time Statistics Page 34

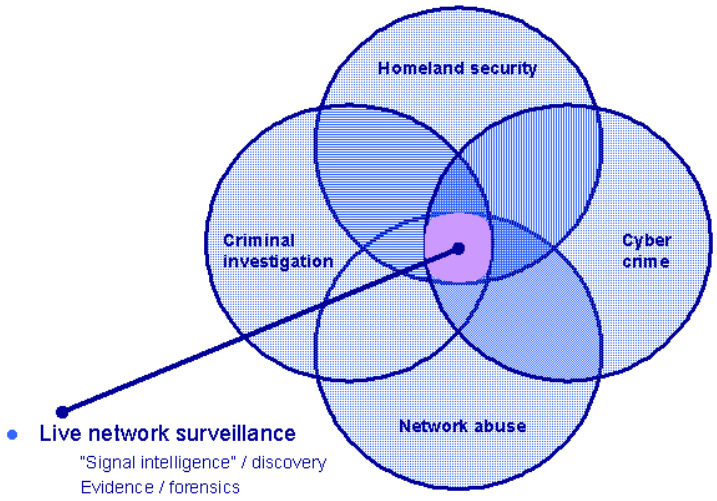
Table of Tables

Table 1. Accepted Value Formats 40
Table 2. Classification Operators Listing 41

 Copyright © IP Fabrics, Inc. 2007

1 Introduction

DeepSweep™ is a live network surveillance device for use in law enforcement, enterprise security, network monitoring, and national security applications. There are many aspects to each of these disciplines. DeepSweep™ helps with evidence gathering and/or criminal/terrorist activity discovery on a live network.



DeepSweep's internal host processor and multi-core packet inspection accelerators allow it to monitor multiple 1Gbps Ethernet links (DeepSweep™-1 model) at true wire-speed with full layer2-7 inspection capabilities.

This manual is intended to serve as a user interface and operational reference, as well as a tutorial.

Chapter 2 provides the operational overview for DeepSweep™. This chapter provides the reader with a general overview of how DeepSweep™ works and its capabilities.

Chapter 3 provides information on how to install DeepSweep™ network surveillance environment.

Chapter 4 provides detailed reference information for how to use DeepSweep™ including the overall format of the DeepSweep™ web pages, how user accounts are made and managed, and detail on each configurable entity on the user interface pages. This section can be consulted if there are questions regarding what a specific configuration option does. This chapter also discusses how to make evidentiary records for use in a court of law.

Chapter 5 describes how advanced users can make their own Linux programs to run on DeepSweep™ for customized processing of packets that DeepSweep™ finds.

DeepSweep™ users can also create classification and patterns databases for use by the surveillance system to identify packets. Chapters 6 and 7 provide information on how to make these databases and load them onto DeepSweep™ for use in a surveillance system.

Chapter 8 lists some of future enhancements (inclusive but not limited to) of the system.

Chapter 9 lists the accounts and port information in the DeepSweep™ system.

 Copyright © IP Fabrics, Inc. 2007

2 DeepSweep™ Overview

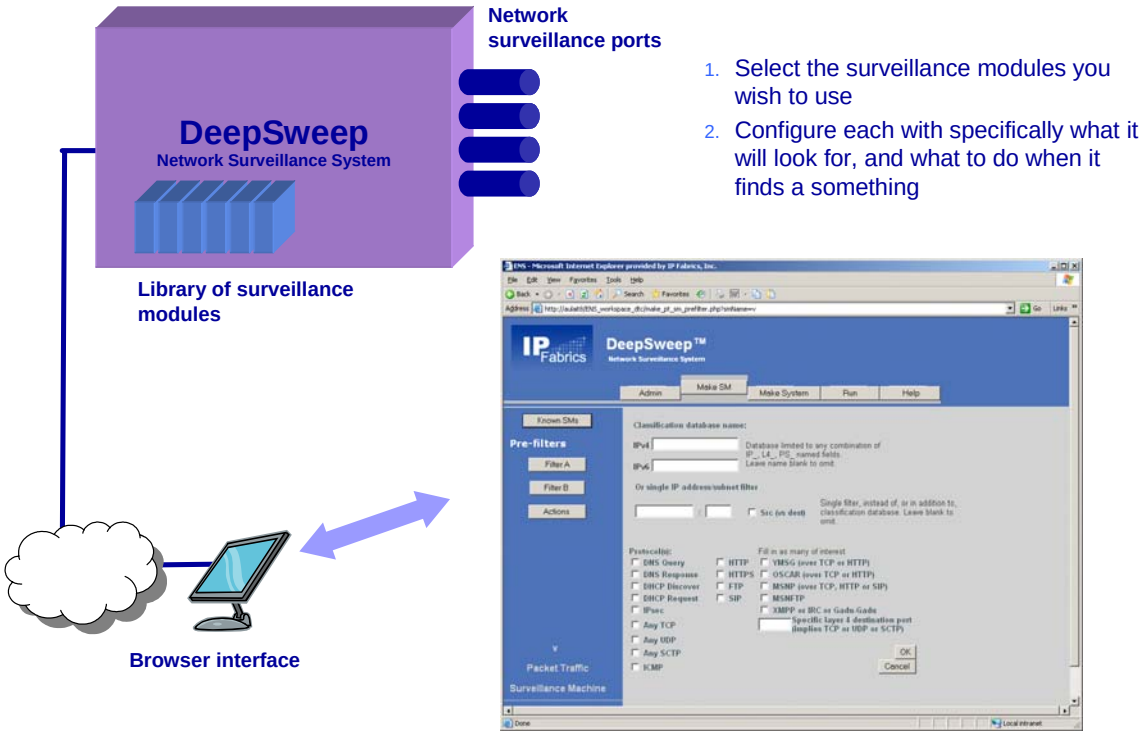
DeepSweep™ is designed to connect with up to eight gigabit interfaces. Installation instructions can be found in Chapter 3, DeepSweep™-1 Installation.

Once installed, DeepSweep™ can be set up for a wide and growing range of network surveillance activities. DeepSweep™ is configured through a web browser interface to look for specific features in the traffic – anything from low level Internet Protocol (IP) addressing and IP address assignment information up to strings and regular expressions that may be found in the content of a packet. It is recommended that if possible, the screen on the monitor on which the browser is being viewed be set to a 1280 X 1024 resolution or higher for optimal viewing.

DeepSweep™ is available with a growing set of ***Surveillance Modules*** (SM). A Surveillance Module is a single functional block that can be configured to perform a specific task in the system. Each Surveillance module is configurable through a web browser. The configuration tells the surveillance machine:

1. What it should be looking for
2. When it finds what the user is looking for, what actions should be taken.

Surveillance Modules can be chained together into a ***Surveillance Assembly*** (SA). A Surveillance Assembly maps DeepSweep™ gigabit input ports to Surveillance Module chains that will perform the processing. Once a Surveillance Assembly is defined, the DeepSweep™ user can then run the assembly using a web browser.

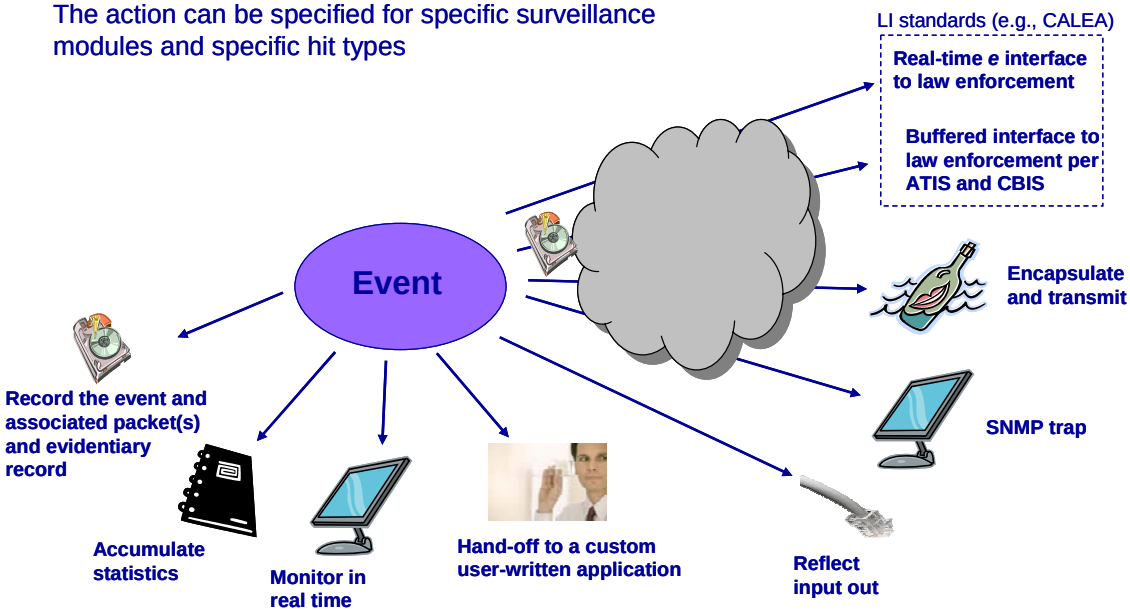


When DeepSweep™ is running a Surveillance Assembly, each surveillance module in the assembly begins processing packets looking for the characteristics configured for the surveillance mission. When a Surveillance Module finds a packet that matches the criteria, this criteria match is called a ***hit***.

 Copyright © IP Fabrics, Inc. 2007

DeepSweep provides a flexible set of action choices when a hit is detected.

The action can be specified for specific surveillance modules and specific hit types


LI standards (e.g., CALEA)
Real-time e interface to law enforcement
Buffered interface to law enforcement per ATIS and CBIS
Event
Encapsulate and transmit
SNMP trap
Record the event and associated packet(s) and evidentiary record
Accumulate statistics
Monitor in real time
Hand-off to a custom user-written application
Reflect input out

Up to three ***hit types*** may be defined by a given Surveillance Module. Through the web browser, DeepSweep™ can be configured to take one or more of a variety of actions on each hit type:

1. **Record**. Generate a record file and log part or all of the packet along with the type of hit and timestamp information. This record file can then be retrieved and used for research or evidence.
2. **Accumulate Statistics**. Through the web browser, a statistics page will show each surveillance module in the surveillance assembly along with how many packets were processed & how many of each hit type was identified in that surveillance module.
3. **Monitor**. The web browser can be used to display hit information messages in real-time so investigators can be notified of hit activity in real-time.
4. **Hand off ("kick") to User Program**. Advanced processing executables can be loaded onto DeepSweep™ and packets causing hits can be forwarded to the program. For more information on this advanced topic, see section 6.
5. **Reflect**. Send an exact copy of the packet out an Ethernet port.
6. **Send SNMP Trap**. Send an SNMP Trap to an SNMP management station.
7. **Encapsulate and transmit**. This action will cause DeepSweep™ to send the packet and hit information to a remote computer.
8. **Legal Intercept (*e.g. CALEA*)**. The DeepSweep supports several direct or buffered CALEA standard interface formats.

Configuring DeepSweep™ occurs through a web browser interface. The following steps are performed to get DeepSweep™ up and running for your application:

1. Navigate to the DeepSweep™ home page located at https://< IP address> (or http:/localhost if locally attached)
2. Use the IP Fabrics supplied username and password to log into the DeepSweep™. This logs you into the admin page of the system.

 Copyright © IP Fabrics, Inc. 2007

3. CHANGE YOUR PASSWORD for this account from this page!
4. Add any users for the DeepSweep™.
5. Configure your Surveillance Module(s). This is done by selecting the "Make SM" tab on the web page. On the main Make SM page, you:
    a. Create a new SM name and assign a Surveillance Module type for it.
    b. Edit the SM name and navigate through each page of the Surveillance Module (buttons on the left) to configure the Surveillance Module for proper operation (for more information on the specific pages, see the specific SM Users Manual).
    c. Select "OK" after configuration of each page is completed or your settings will not be saved!
6. Configure the Surveillance Assembly. This is done by selecting the "Make SA" tab on any web page. On the main Make SA page, you:
    a. Create the new SA name.
    b. Use one of the Connections pages to map Ethernet inputs and outputs to ***packet inspection accelerators*** (PIXLs). This page also lets you specify how packets flow through the DeepSweep™ for optimal performance of your application.
    c. Use the SM chains page to configure SM chains for each PIXL used for the application.
    d. Use the SM actions page to configure what actions will be taken for each hit type of each SM used in the Surveillance Assembly.
    e. Use the SA Options page to configure SA-global parameters.
7. Go to the Run/Control page by selecting the Run tab. From here, you can select the Surveillance Assembly to run, then start and stop the assembly by using the "Start" and "Stop" buttons. Status of the DeepSweep™ will be shown in the status box on the bottom half of the Run/Control page.
8. Real-time monitor information can be viewed on a running DeepSweep™ by selecting the "Monitor" button on the left side of the Run page. This will show a scrolling list of hits and which SM is generating the hit in real-time. This page can be paused and resumed for easier viewing.
9. Statistics information can be viewed on a running DeepSweep™ by selecting the "Statistics" button on the left side of the Run page. The statistics page has a reset button that will reset all counters in real-time.

Some surveillance modules may use special ***classify*** or ***patterns databases*** for operation. Information on creating these databases can be found in sections 4.3.6.1 (Classify Database) and 4.3.6.2 (Patterns Database). Once created, these databases are loaded onto the DeepSweep™ by establishing a secure FTP session (i.e. using WinSCP for example) to the DeepSweep™. There is a single directory there to which databases can be loaded onto the DeepSweep™. These databases can also be dynamically updated during operation. More information can be found in section 4.3.2.

If user programs are written for operation on DeepSweep™, they are loaded to the same directory as the databases. Refer to section 5, Creating User Defined Programs for DeepSweep™ for more information.

Record files for a given surveillance assembly run can also be found in this directory. Each record file(s) will contain the date and time as part of the file name. Using secure FTP, this record file can be loaded onto a remote machine and deleted from the DeepSweep™.

DeepSweep™ also generates evidentiary records which provide all specific configuration information for the surveillance assembly that was run along with a digital signature to ensure the information has not been tampered with. These records are also found in this directory. Once the surveillance assembly has been stopped, evidentiary records can be loaded via secure FTP to remote hosts for use as supporting information for the integrity of the network monitoring evidence.

The DeepSweep™ logs keep track of users that logged into and out of the system, when SAs were run, stopped, etc. This log can be viewed through an SSH session to the DeepSweep™. If the current log file needs to be moved to a remote machine, use the "start new log" file on the administration page to save the current log and start a new one. The newly saved file can then be loaded onto a remote host for use.

 Copyright © IP Fabrics, Inc. 2007

3 DeepSweep™-1 Installation

3.1 Hardware Setup

The front view of a DeepSweep™-1 unit is shown in Figure 1 below. The power switch is on the front panel. There are no cable connections made to the front of the unit.

Figure 1. DeepSweep-1 front view

All cable connections are made on the rear of the system. This is shown in Figure 2.

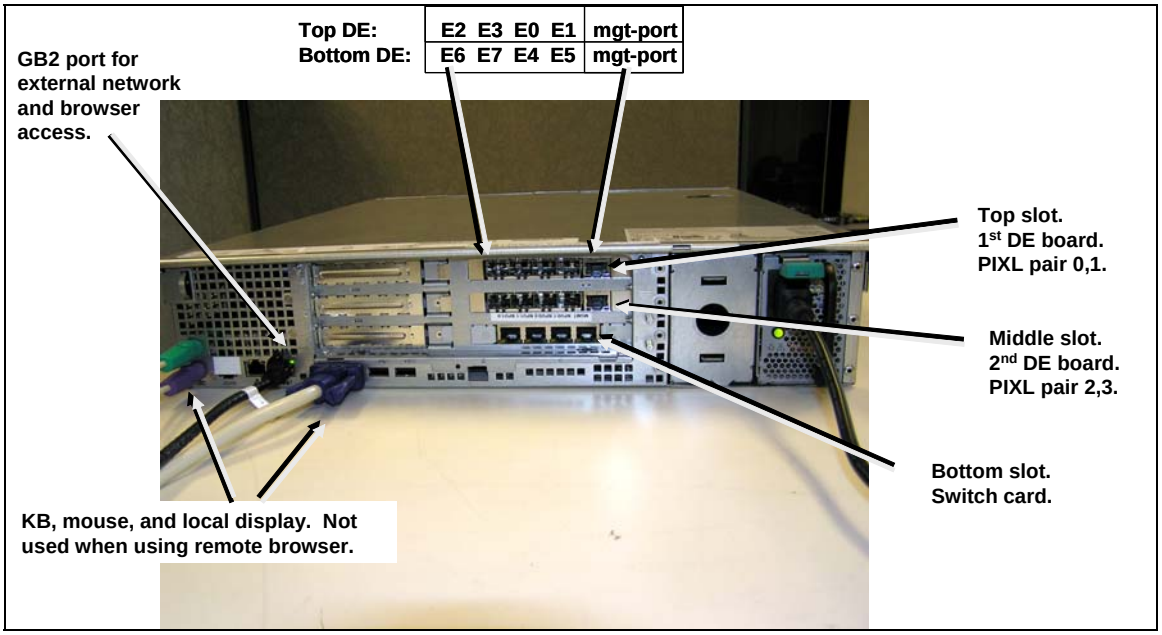

Top DE: E2 E3 E0 E1 mgt-port
Bottom DE: E6 E7 E4 E5 mgt-port
GB2 port for external network and browser access.
Top slot. 1st DE board. PIXL pair 0,1.
Middle slot. 2nd DE board. PIXL pair 2,3.
Bottom slot. Switch card.
KB, mouse, and local display. Not used when using remote browser.

Figure 2. DeepSweep-1 rear view

The "mgt-port" connections are used for intra-system connectivity and must be connected as shown in Figure 3.

 Copyright © IP Fabrics, Inc. 2007

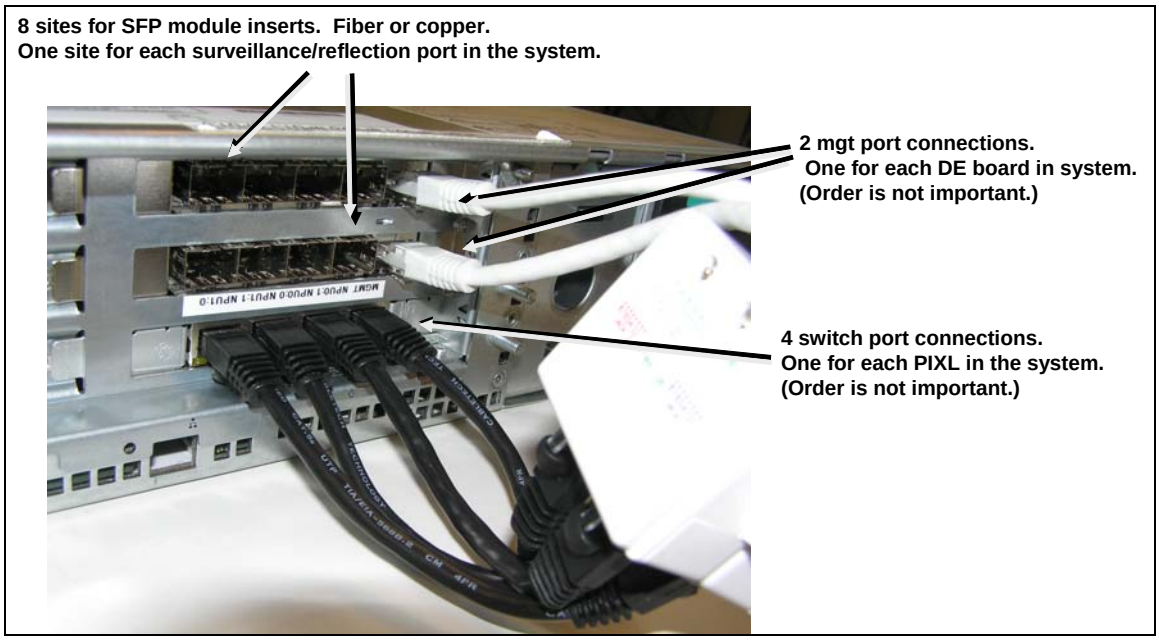

8 sites for SFP module inserts. Fiber or copper.
One site for each surveillance/reflection port in the system.
2 mgt port connections.
One for each DE board in system.
(Order is not important.)
4 switch port connections.
One for each PIXL in the system.
(Order is not important.)

Figure 3. Mgt-port to switch connections

If your system is not set up by IP Fabrics personnel then you may need to install the Double Espresso (DE) boards and the switch card yourself. If you are installing two DE boards then you must install them in the correct slots. Each board will be marked to indicate the correct slot – top, middle or bottom. If you have a single DE board then it must go in the top slot. To install the board:

1. Ensure that the system is not running and remove the power cord.
2. Remove the top cover of the unit. Push blue button on the top and slide the cover to the rear of the unit.
3. Remove the card cage vertically using the two blue latches shown in Figure 4.

Figure 4. Top view with cover removed.

4. Carefully insert the DE and switch cards as shown in Figure 5

 Copyright © IP Fabrics, Inc. 2007

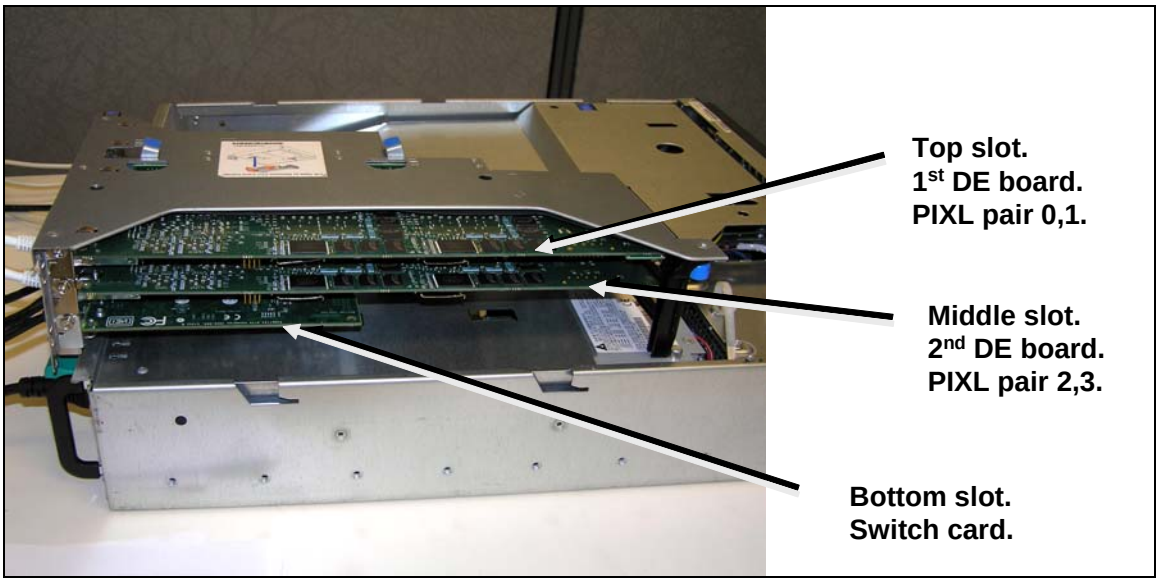


Figure 5. Side view with card cage elevated

5. Re-seat the card cage.
6. Re-install the top cover.
7. Connect the power cord.

3.2 DeepSweep™ Power-up and initial configuration

Once the hardware is set up just press the power-on button and the system will boot up to its pre-configured state. If you plan to use a directly attached keyboard, mouse and display then all should be ready. If you plan to connect to your own private network then you will need to connect the network cable to port "GB2" and show above. As pre-configured, the system will have a static IP address assigned. Normally, you will need to change this to conform to your own network environment. The System Interface" page will report the information for the external "system ports" (i.e. "GB1" and "GB2") and allows the "admin" account to change the configuration.

Launch a browser and point it to the DeepSweep login page. If running locally then click the browser icon at the top of the desktop page and it will go to the initial screen. If running over a network connection (via "GB2") the use HTTPS with the IP address or name you assigned to the DeepSweep-1.

For example, if you assigned an IP address of 192.168.43.50 then you would enter:

https://192.168.43.50

3.3 DeepSweep™ Use with a Network Tap

If using an Ethernet tap (copper or fiber) to acquire the traffic stream to monitor then you connect to desired ports (e.g. E0 and E1) to be able to see data in each direction. Use could use a single port such as E0 if you want to look at traffic in a single direction. In either case, follow the screen configuration descriptions for setting up your required Surveillance Modules (SM) and Surveillance Assembly (SA). This is described further in section 4.3.3 on Surveillance Assembly configuration..

 Copyright © IP Fabrics, Inc. 2007

3.4 DeepSweep™ Use with a Single Traffic Stream

If using an external hub or switch span/mirror port to provide the traffic data stream then it will likely be adequate to use a single input port – E0. See section 4.3.3 on Surveillance Assembly configuration.

3.5 Firewall settings - "iptables"

Upon initial system setup please confirm that the firewall settings work for your particular installation environment. The DeepSweep uses a standard Linux "iptables" firewall. The firewall discards unwanted traffic and generally protects the DeepSweep from unauthorized access.

The default configuration allows all incoming HTTPS, NTP, SNMP, SSH traffic and (local only) HTTP. It also allows limited incoming ICMP traffic (up to 10 ICMP requests per second). Depending on your installation, you may need to change the firewall configuration. For example, you may wish to allow only incoming connections from a list of known management hosts.

The default firewall configuration also accepts all traffic to/from the PIXL's that exist on internal connections that are private to the DeepSweep and allow all outgoing connections (i.e. 192.168.100.101 through 192.168.100.103). This behavior is required for the DeepSweep to function properly. **Do not change these settings**.

The iptables chains are broken into three pieces:

- The "INPUT" and "OUTPUT" chains allow the "core" DeepSweep operation (SSH, SFTP, buffering, etc);
- The "DYNAMIC_INPUT" chain implements the configuration accessed via on the security page;
- The "USER_INPUT" and "USER_OUTPUT" chains allow the user to do site-specific customization.

The system administrator must *not* modify the first two chains, since this potentially interferes with the normal system operation.

The administrator can add/delete/modify the rules in the USER_* chains if required. The default ingress/egress policies reject *all* traffic, so the administrator can open holes by adding rules to the chain; or close them by removing rules. Rules in the USER chains are applied only after the rules on the other two chains have not-matched the packet.

The default USER_* chains enable ICMP, SNMP + NTP, since none of these are (currently) critical to the system operation.

If the firewall setting are to be changed then by follow the steps below. A basic understanding of the "iptables" software is required to make these changes. A reference example file can be found in Appendix A –'iptables' reference firewall file.

1. Login (Linux) to the DeepSweep as "root".

2. At the Linux command prompt, type:
   `/sbin/service iptables stop`

3. Edit the file `/etc/sysconfig/iptables` as desired.

4. At the Linux command prompt, type:
   `/sbin/service iptables start`

3.6 Time Synchronization – "NTP"

The DeepSweep uses NTP to maintain an accurate clock.

 Copyright © IP Fabrics, Inc. 2007

By default, the DeepSweep relies on the US public NTP pool as its NTP source. The DeepSweep thus requires DNS access and a route to the external Internet. If you wish to use a different NTP source or do not have DNS available, you will need to change the NTP configuration.

You can change the NTP settings by following the steps below. You will need a basic understanding of the Linux NTP daemon software to make these changes. A reference example file can be found in Appendix B –'ntp.conf'reference file.

1. Login (Linux) to the DeepSweep as "root".

2. At the Linux command prompt, type:
```
/sbin/service ntpd stop
```

3. Edit the file `/etc/ntp.conf` as desired. Typically, you will only need to edit these three lines:
```
server 0.us.pool.ntp.org
server 1.us.pool.ntp.org
server 2.us.pool.ntp.org
```

4. At the Linux command prompt, type:
```
/sbin/service ntpd start
```

After restarting the NTP service, the DeepSweep may require several minutes before it synchronizes with your new NTP source.

The DeepSweep will still operate correctly if it has no NTP source, at the cost of less clock accuracy.

 Copyright © IP Fabrics, Inc. 2007

4 Using DeepSweep™

4.1 General DeepSweep™ Configuration Page Layout

Before going through the details of the DeepSweep™ configuration pages, let's take a look at the general layout for all the pages so it's easier to navigate.

All DeepSweep™ pages have the same general format as shown in the page displayed in Figure 6. There are three sections that are on all pages:

- The DeepSweep™ Configuration tabs across the top of the configuration area. Each tab represents a step in the configuration and operation of a surveillance assembly on DeepSweep™.
- DeepSweep™ configuration pages for each tab appear on the left side of the page.
- Buttons that control submitting the configuration. The "OK" button submits the configuration defined on the page. Selecting "Cancel" (or leaving the page without selecting "OK" does not save any configuration changes made to the page.

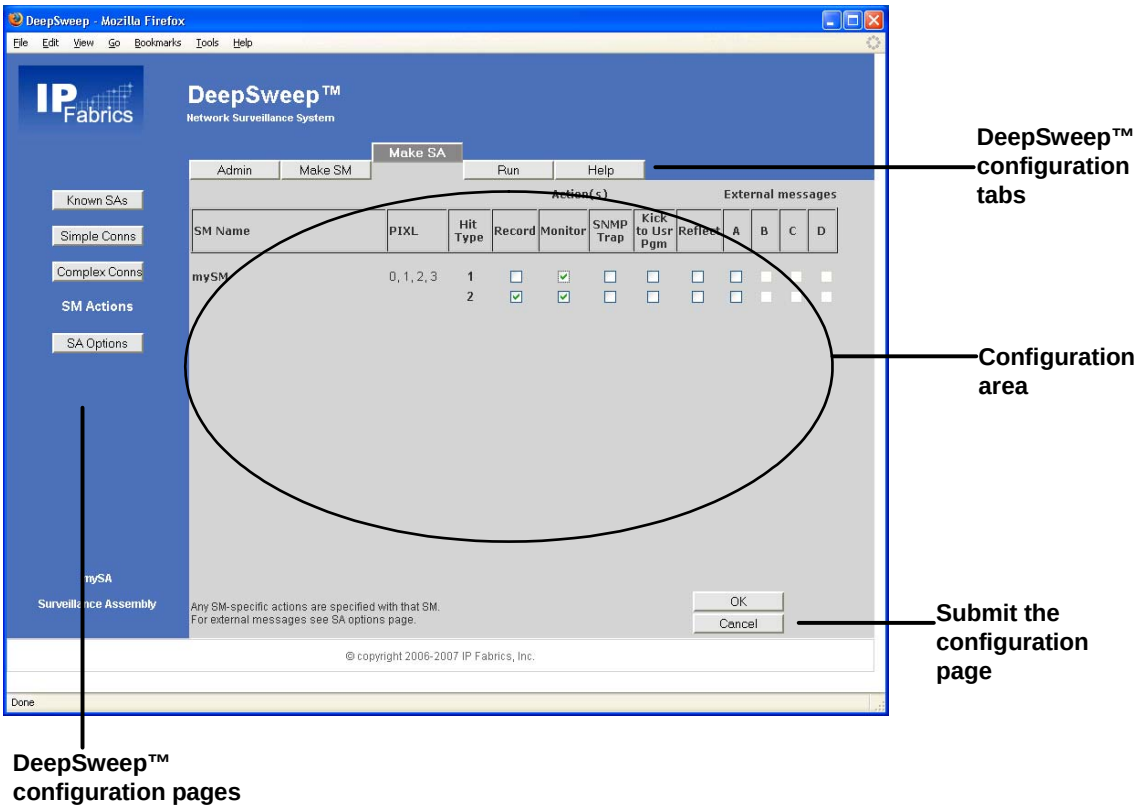


Figure 6. DeepSweep Page Layout

There are five DeepSweep configuration tabs across the top – **Admin**, **Make SM**, **Make SA**, **Run**, and **Help**. Each of these tabs and their associated pages will be described later. You can tell which configuration tab you are on by looking at the tabs – the tab that is raised above the others with a darker shade is the configuration tab page currently being displayed. In the case above, this is the "Make SA" tab.

The column of buttons on the left side of the page provide access to all pages for that tab. You can tell which page is being displayed because it is no longer a button and the text is in white. For example, in Figure 6 we're on the "SM Actions" page. The other pages for this category can be accessed by selecting the corresponding button along the left side of the page. For example, if we wanted to go to the one of the connections pages, we would simply click on the **Simple Connections** button on the left and we would be taken to the Make SA Connections page. In this document we will use the general term **Connections** to mean one of the two connections pages.

 Copyright © IP Fabrics, Inc. 2007

The things that can be configured on a given page will be in the center grey area of the page. These may be text boxes, scroll down menus, check boxes, etc. Once you have entered all the configuration information for that page, you must select the "OK" button**. If you perform some configuration on a page, then go to another page without clicking "OK", your configuration information will be lost.** Likewise, clicking on the cancel button will restore the last committed configuration for the page.

In summary, select the tabs across the top to go through each phase of building a surveillance assembly. Select the boxes along the left column for each tab to go to a specific page within that category. Then when configuration of a page is completed, make sure you click "OK" to submit the configuration. If you don't want to save your configuration work for the page, click the "Cancel" button or simply leave the page.

4.2 User Accounts and Account Management

In the DeepSweep™ system, each account is identified by a unique id. To use the system you need an account/id along with the associated password for that account/id. In the following sections we will use account and user id interchangeably unless otherwise mentioned.

The DeepSweep™ system comes preconfigured with an administrator account user ID("admin") and default password ("ipfabrics") provided by IP Fabrics. By accessing the system using this account, user accounts can be setup for individual users. Only the administrator account has the ability to create accounts, delete accounts, and change passwords for user accounts.

The following sections cover the administration and account management pages and their associated sections.

Figure 7 shows the DeepSweep™ login page.

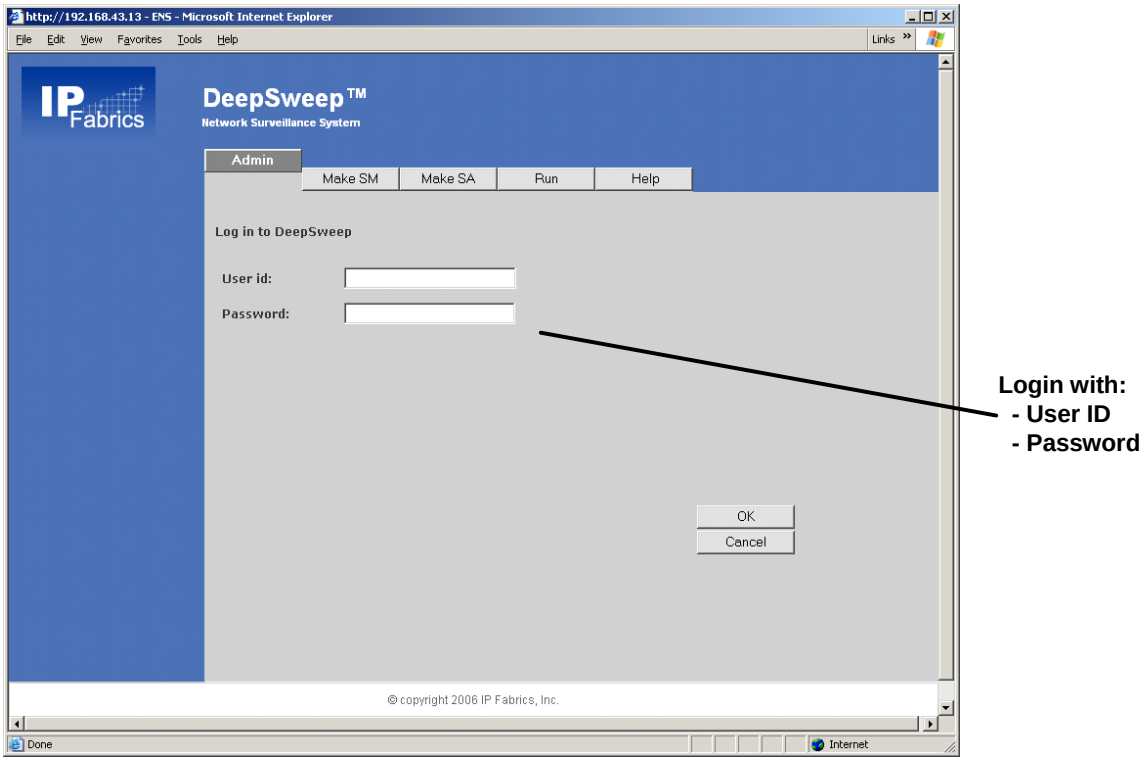


Figure 7. Login Page

Once the DeepSweep™ administrator has entered the proper credentials and pressed the "OK" button, the administration account management page will be displayed (Figure 8). This page is specific to the administrator account and has five different sections – logout, change password, add user, system log/file management and delete user/change password.

The logout section allows the administrator to logout of DeepSweep™ by clicking on the Logout button.

 Copyright © IP Fabrics, Inc. 2007

The change password section allows the administrator to change his or her password. The old password and the new password are required in order to successfully change the password. The result of the operation will be displayed in a message below the **Change Pswd** button indicating the success/failure of the operation. It is highly recommended that the administrator account's password be changed from the default password when the administration user first logs into the system.

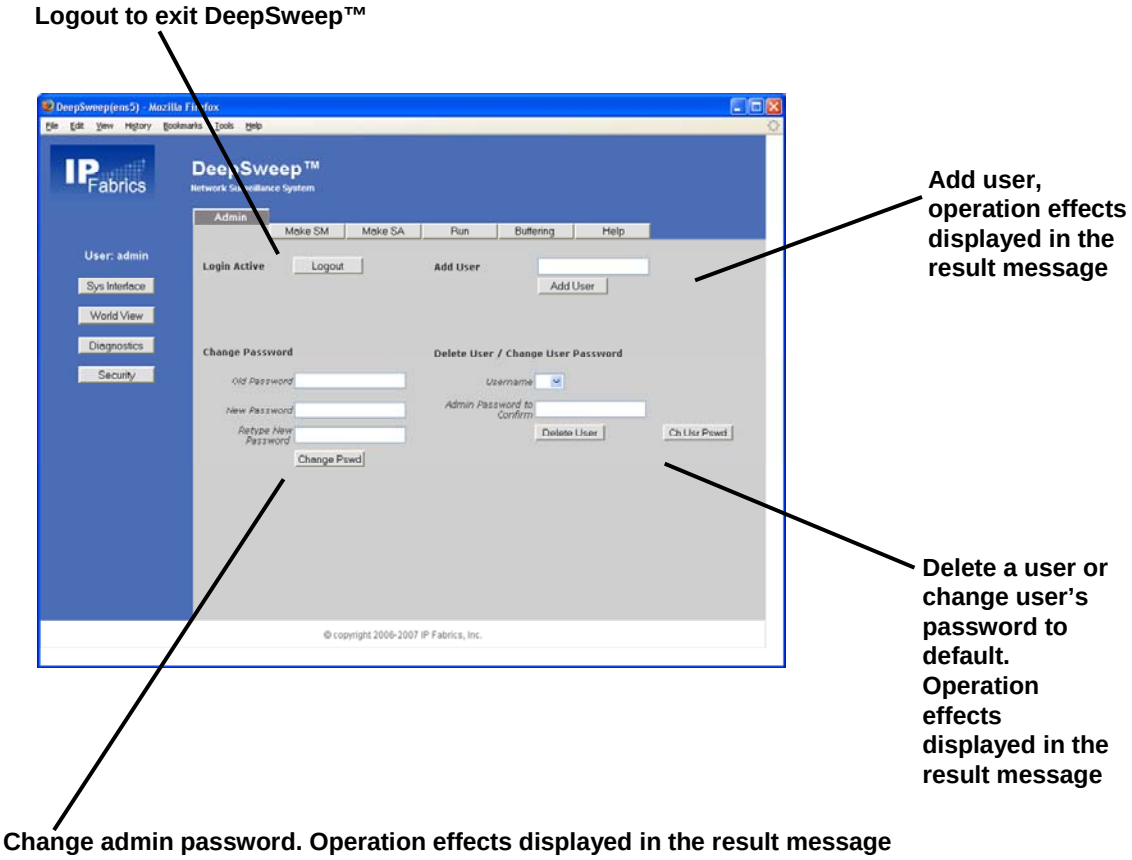


Figure 8. Admin Account Management page

Logging in as the administrator account with the username and password provided by IP Fabrics takes the administrator to the admin page. This page allows the administrator to create new user accounts. Each user id must be unique and is created with the default password ("ipfabrics"). The result of the operation will be displayed in a message below the **Add User** button, indicating the success/failure of the operation.

The delete user/change user password section allows the admin to manage user accounts. A user account can be deleted or the account's password can be reset to the default password using the appropriate buttons. The result of the operation will be displayed in a message below the **Delete User** and **Ch Usr Pswd** buttons, indicating the success/failure of the operation.

Logging in as a non-administrator will also take you to the admin page shown in Figure 9 below. The non-admin account user's view of this page contains less configuration information. From the user admin page, the user has the ability to logout of their session and change the password for the account and start a new system log (while retaining the previous logs).

NOTE: It is highly recommended that the user change his or her password after logging in for the first time and periodically there afterward.

 Copyright © IP Fabrics, Inc. 2007

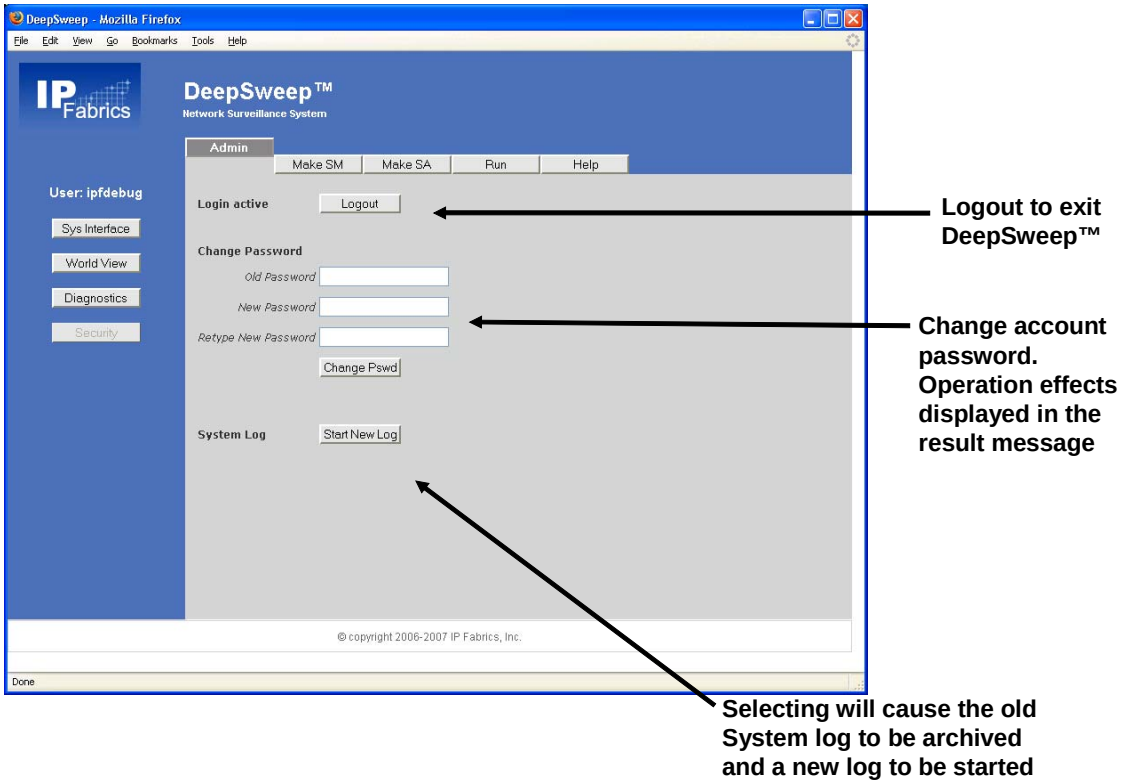


Figure 9.User Account Management page

4.3 Operational Overview

4.3.1 Administration Pages

There are four additional administration pages – System interface, World View, Diagnostics, and Security.

4.3.1.1 System Interface Page

The System Interface page enables the DeepSweep™ user to configure the standard internet connectivity information for each of the two system interface ports available on the DeepSweep™. Figure 10 shows the contents of the page. When installing DeepSweep™ to pass information over the system interface, contact the network system administrator for IP address, netmask, and default gateway information for each management port used.

 Copyright © IP Fabrics, Inc. 2007

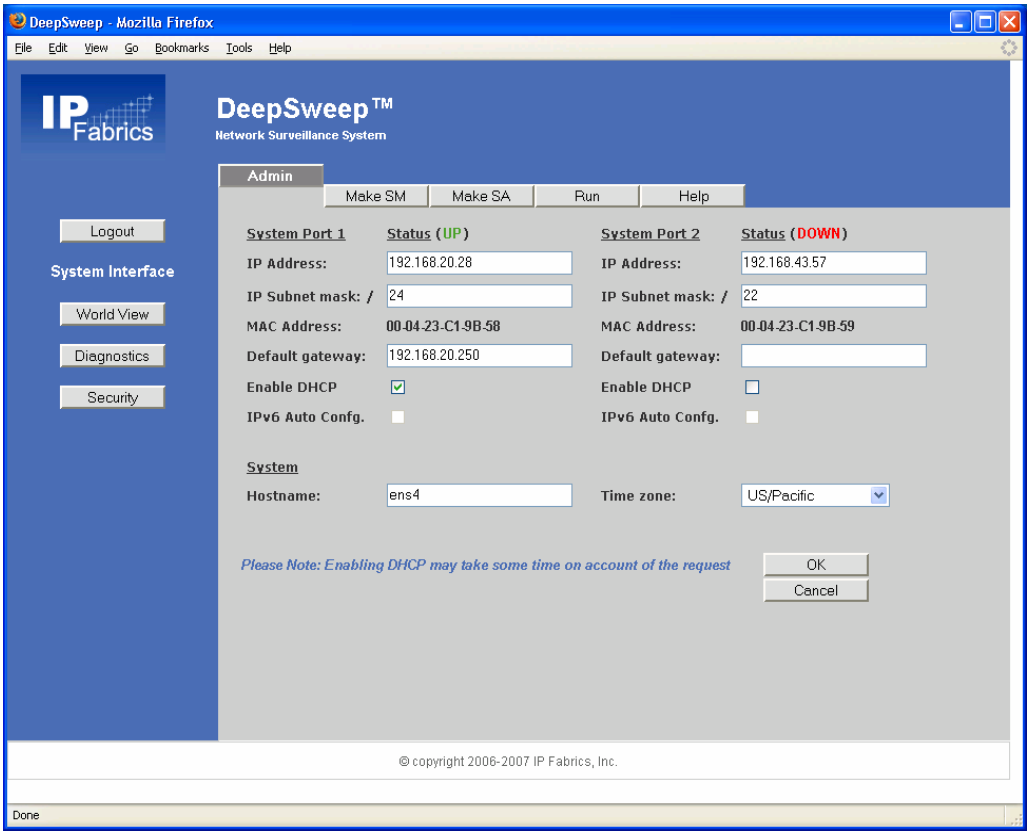


Figure 10. Administration Tab, System Interface Page

4.3.1.2 World View Page

The world view page is shown in Figure 11. This page configures global DeepSweep parameter information.

DeepSweep has the ability to report traffic hits through SNMP Traps. If this action is to be used in your system, you must provide the IP address of the trap recipient for any SNMP traps that may occur during execution. (Note: You must also click the "SNMP Trap" checkbox on the SM Actions page as part of the SA definition.)

You may also enable SNMP traps for other system notifications. Each of these is selectable individually. Please refer to the separate document "DeepSweep Alerts" for a more in-depth discussion of this feature and its use.

 Copyright © IP Fabrics, Inc. 2007

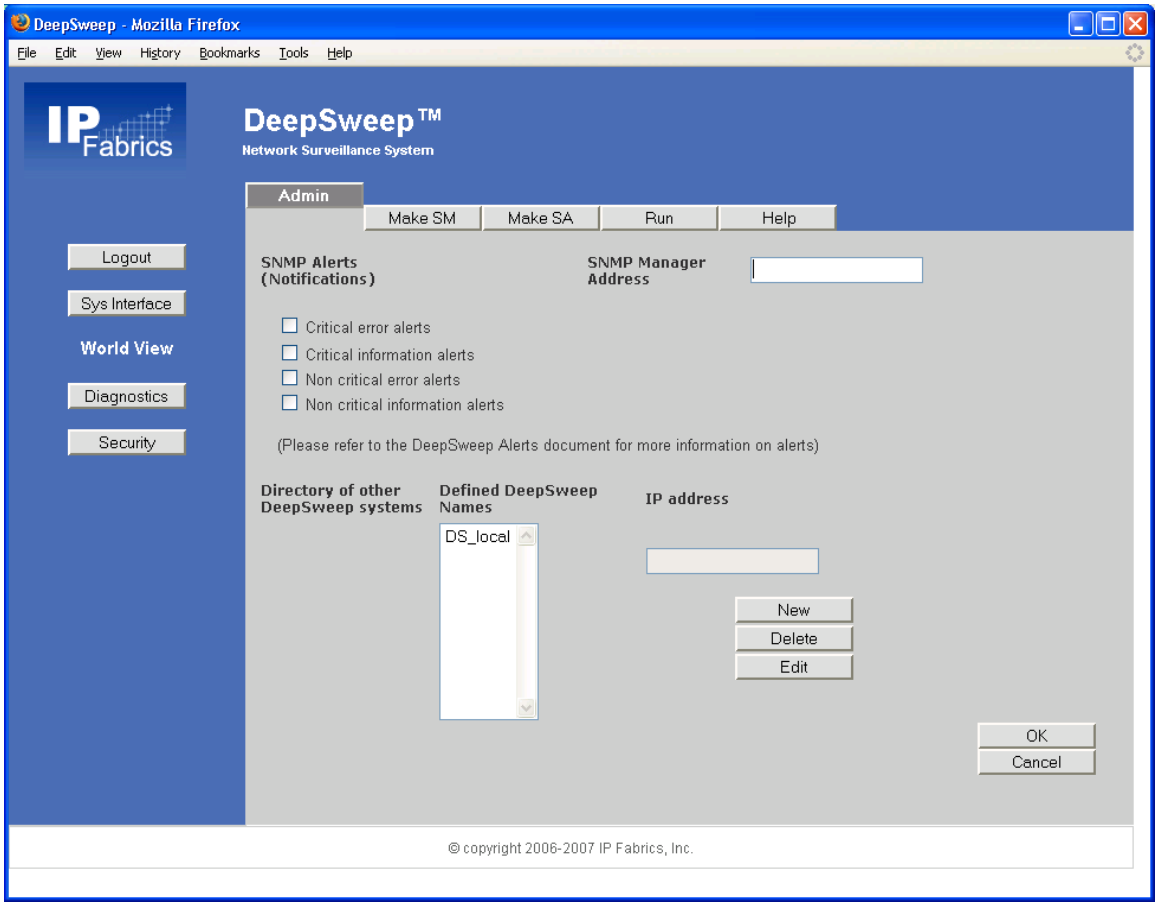


Figure 11. Administration Tab, World View page

4.3.1.3 Diagnostics

This page has restricted access. The "admin" account always has access to Diagnostics. As shipped, this is the only account that has this access. If desired, the administrator may create an account named "ipfdebug". This account name is the only other account that is ever given access to the Diagnostics page. This account is not required unless you are working with IP Fabrics technical personnel.. As always, if you do create this account than you should be sure to change its default password to keep the system secure.

The Diagnostics page access should be carefully managed and controlled.

4.3.1.4 Security Page

This page is accessible only by the "admin" account. The page is used to set (restrict) external access via the two System Ports and for some global file system maintenance.

There are four File system buttons:

- Start New Log – Starts a new system log. This will cause the current system log to be closed and a new system log to be started.
- Delete Log Files – Starts a new "systemlog" and deletes/clears all other log files.

 Copyright © IP Fabrics, Inc. 2007

- Delete Run Files – Deletes/clears all runtime output files such as Record files, Evidentiary Record files and any other internal file that system may have used as working space during execution of a Surveillance Assembly ("SA").
- Cleanse System – Deletes/clears files to restore the system to nearly state it was upon installation. This includes all log files and runtime files. Additionally, it deletes any databases in the FTP area and deletes all user configuration information including all SMs and SAs. This button requires a double-confirmation and then is final. **Use with care! It cannot be reversed.**

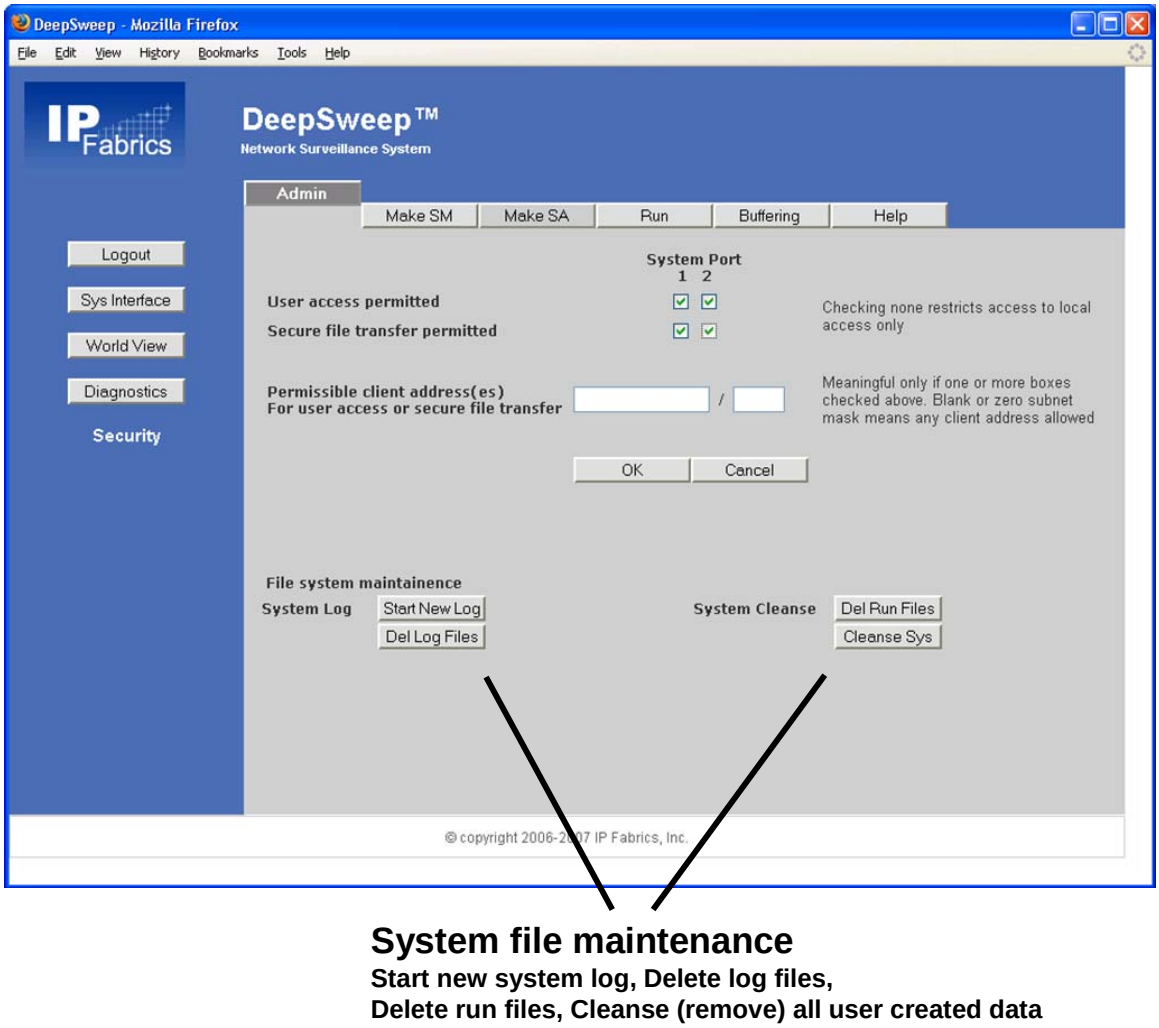


Figure 12. Administrative tab, Security page

4.3.2 Run Pages

Before getting into the specifics of surveillance assemblies and surveillance modules, let's cover the run pages.

- The run pages are accessible by selecting the **Run** tab on any DeepSweep™ page. These pages allow the DeepSweep™ user to control operation of the DeepSweep™, i.e. run a surveillance assembly, stop a running surveillance assembly, and pause or resume a running surveillance assembly.

 Copyright © IP Fabrics, Inc. 2007

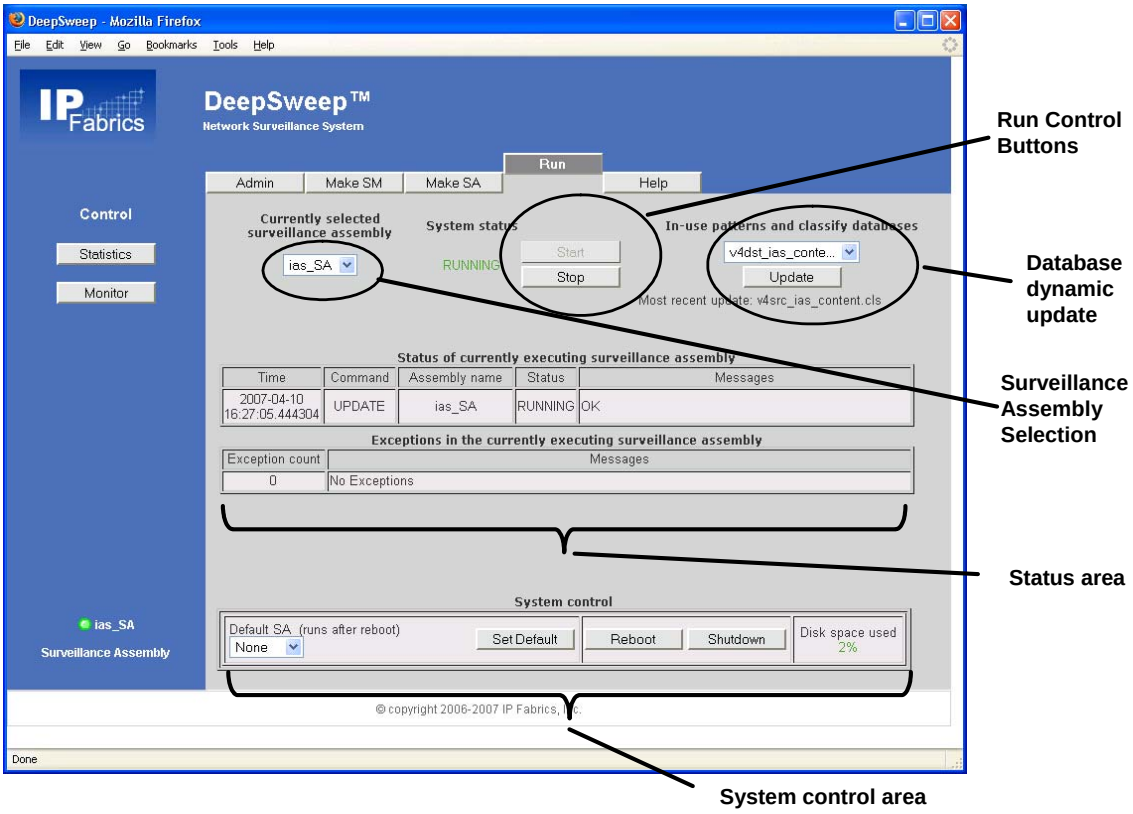


Figure 13. Run Page

There are three main pages to the DeepSweep™ run operation:

- **Control**. The control page allows the user to select the SA to run from a pull-down menu of defined surveillance assemblies (SAs are managed using the **Make SA** tab). Once selected from the pull-down list, the control buttons can be used to start and stop surveillance assembly operation. Any patterns or classify databases used with the SA will appear in the pull-down menu. If any of these databases need to be updated during execution, load the new database into the user area and select the "Update" button on the run control page to perform the database update. The status area below the control area displays the current operational status of DeepSweep™ and an exception count if any anomalies have occurred during operation. When a command is selected, the page will refresh periodically until the operation has been executed. During this time you can see the current status of DeepSweep™ as it executes the command.
- **Statistics**. The statistics page provides information on each surveillance module in the surveillance assembly. For more information on the statistics page, see section 4.3.5.6.
- **Monitor**. The monitor page displays hit information in real-time. For more information on the monitor page, see section 4.3.5.3.

4.3.3 Surveillance Assembly Pages

A Surveillance Assembly is a distributed set of processing across one through four ***Packet Inspection Accelerators***, or PIXL(s). The more intensive the packet processing is, the more PIXLs are needed to process traffic. This allows DeepSweep to scale performance based on the line rate being processed and the complexity of the inspection going on. So, when creating an SA, you will:

- Determine how to utilize the PIXLs in DeepSweep to optimize performance for the surveillance activity.
- Configure the processing within each PIXL by selecting SMs that will run on each PIXL.
- Configure the actions to be taken when hits are found by each SM used in the Surveillance Assembly.
- Configure Surveillance Assembly global parameters.

 Copyright © IP Fabrics, Inc. 2007

These pages are configured from the **Make SA** tab. The surveillance assembly pages include:

- **Known SAs**. Create, delete, and edit surveillance assembly names.
- **Simple Connections**. Configure inputs and outputs of the PIXLs for the application.
- **Complex Connections**. Additional configuration inputs and outputs of the PIXLs for the application that are available only in an eight-port DeepSweep.
- **SM Chains** (subordinate to the Connections pages). Add SMs to each processing chain in each PIXL used by the SA.
- **SM Actions**. Define actions to be taken when the hit criteria is met for each SM in the SA.
- **SA Options**. Set global configuration options for the SA.

Each of these pages is described in more detail in the sections that follow.

4.3.3.1 Known Surveillance Assemblies (SA) Page

The **Known SAs** page comes up by default when the **Make SA** tab is selected. A list of all known Surveillance Assembly names are displayed on the page.

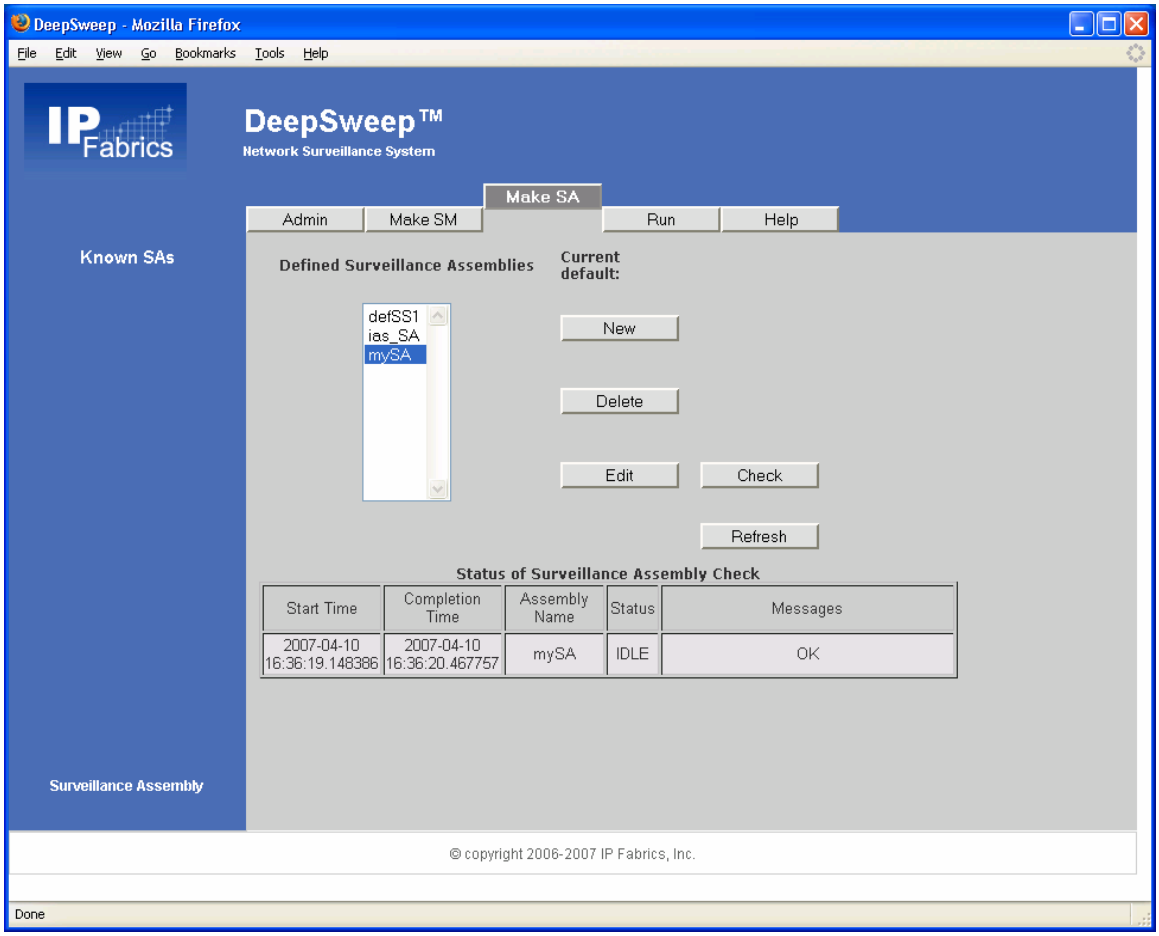


Figure 14. Make Surveillance Assembly Main Page (Known SAs)

Selecting the **New** button will bring up a new page where you can input the surveillance assembly name. This is used as a handle and any alphanumeric name with underscores or periods will work (no spaces!). Once you're done entering the name, select the **OK** button. When you select **OK** (or Cancel) you'll be taken back to the **Known SAs** page. Your newly created SA name will be in the list of SAs on the page. SAs can be deleted by selecting the SA name, then clicking the **Delete** button.

 Copyright © IP Fabrics, Inc. 2007

The **Make Default** button initializes the highlighted Surveillance Assembly as the "default" SA for the device. The default SA is the one that is automatically displayed on the Run tab control page. If configured to automatically start an SA on power-on, the default SA is the one that will be run.

Once the SA name has been created, it needs to be configured. This is done by selecting the SA name from the list and clicking the **Edit** button. The **Edit** button allows existing SA configurations to be changed and/or initialized. Selecting an SA name from the list and clicking on the **Edit** button will take you to the **SM Chains** page (the **SM Chains** page will be covered later).

Once the configuration of an SA has been completed, it can be checked for proper operation by selecting the **Check** button. SAs can be created and checked while DeepSweep™ is operational. When selected, the system will validate the SA selected and status information will be displayed in the status area of the page. The status area on this page does not update automatically and can be updated by clicking on the Refresh button.

4.3.3.2 Connections Pages - Define the Topology

The **Connections** pages determine how traffic is routed through DeepSweep. Figure 15 shows the **Simple Connections** page. Depending on the DeepSweep model number and ports, your page may have one, two or four PIXLs shown. The greater the number of PIXLs you have then the greater the number of topology options are available. The **Simple Connections** are available for all systems but only the first two icon-depicted configurations are available for the 2-port (single PIXL) system. **Complex Connections** are only available for eight-port systems.

Each PIXL consists of two distributor/SM chain pairs (X & Y). The distributor function (small wheel icon) within a PIXL distributes unprocessed traffic between up to three destinations. The distributor will always send traffic to its local SM chain. It may also distribute to other chains depending on the connection topology you select.

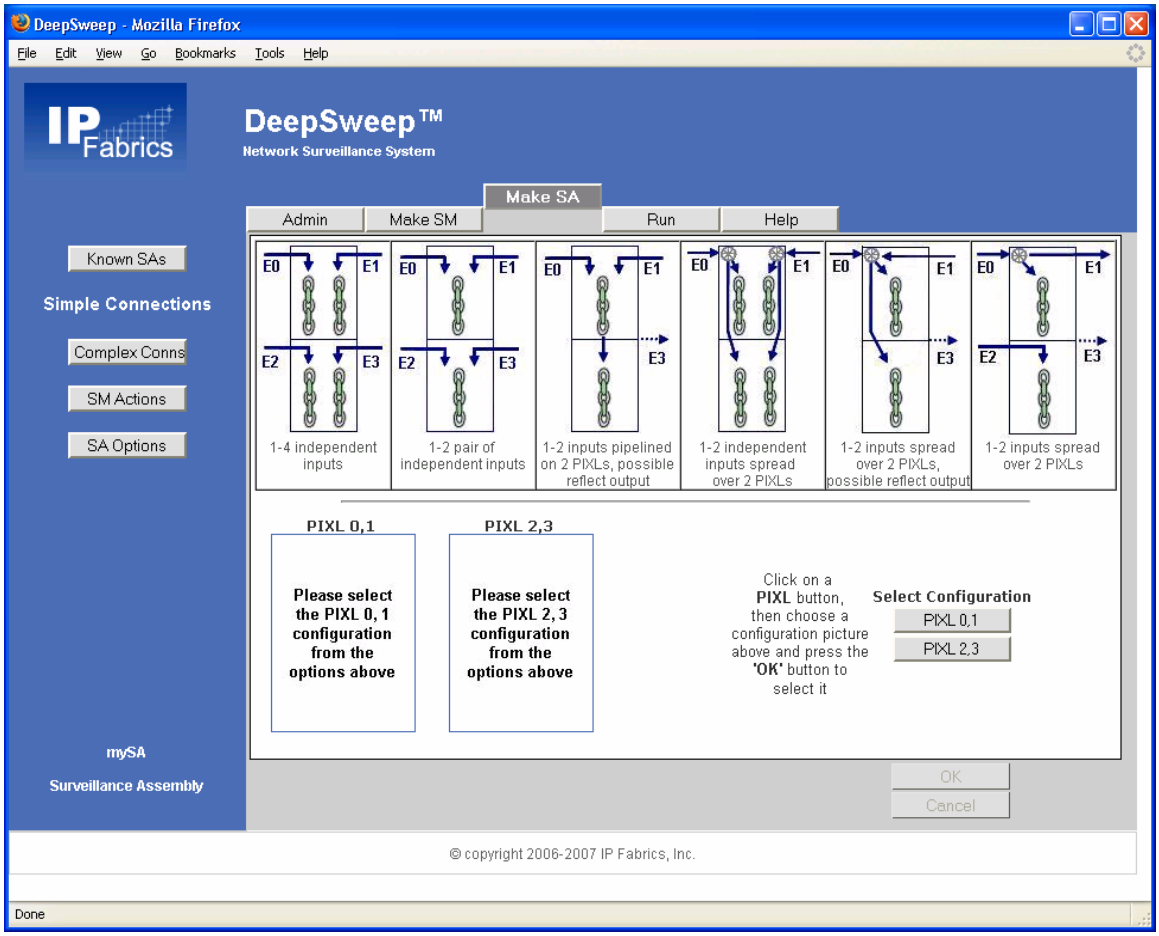


Figure 15. Make SA Tab, Connections Page

PIXL0 is paired with PIXL1 and PIXL2 is paired with PIXL3. The E0 and E4 inputs on PIXLs 0 and 2 can only be used as inputs while the rest of the Ethernet ports can be configured as inputs or outputs. Ethernet ports cannot be configured as bidirectional in the **Simple Connections**.

The solid, dark lines represent raw traffic with the arrow heads depicting direction of (simplex) flow.

The dashed lines represent "reflected" packets. These are packets that match the criteria for a specific SM for which the "reflect" option is checked on **SM Options** page. Any "reflected" packet that is sent out will be exactly the same as the arriving packet prior to analysis – L2 through content. This feature can be used to send hit packets to another PIXL via an Ethernet cable or to some other monitoring computer or equipment.

Figure 15 shows a simple set of configuration options for a DeepSweep. To use this page do the following few operations.

1. Click on the "PIXL 0,1" button (lower left of page) to indicate you want to choose a topology for this first PIXL pair.
2. Click on one of the icons across the top of the page that matches the topology you want.
3. Click on OK. The selected icon will appear on the lower half of the page.

If you have a 2- or 4-port system then you are done. Otherwise, repeat the process for the second PIXL pais (2,3).

1. Click on the "PIXL 2,3" button (lower left of page) to indicate you want to choose a topology for this second PIXL pair
2. Click on one of the icons across the top of the page that matches the topology you want.
3. Click on OK.

The result is shown in Figure 16. **To complete the SA definition you will need to click on each of the PIXL pairs** in the lower part of the screen but first a bit more on the meaning of the topology.

For PIXL 0,1 input traffic comes in through one of the interfaces (E0, E1, E2, E3), the distributor simply passes E0 stream through to its local SM chain X on PIXL 0; E1 to chain Y on PIXL 0; E2 to Chain X on PIXL 1; and E3 to Chain Y on PIXL 1. The diagram is surely simpler than the words. All packets matching the hit criteria will be handled according to the selections for **SA Options** and **SM Actions** for this Surveillance Assembly.

Likewise for PIXL 2,3 except the input ports' streams are merged before sending to the single chain. That is, E4+E5 to the chain on PIXL 2 and E6+E7 to the chain on PIXL3.

 Copyright © IP Fabrics, Inc. 2007

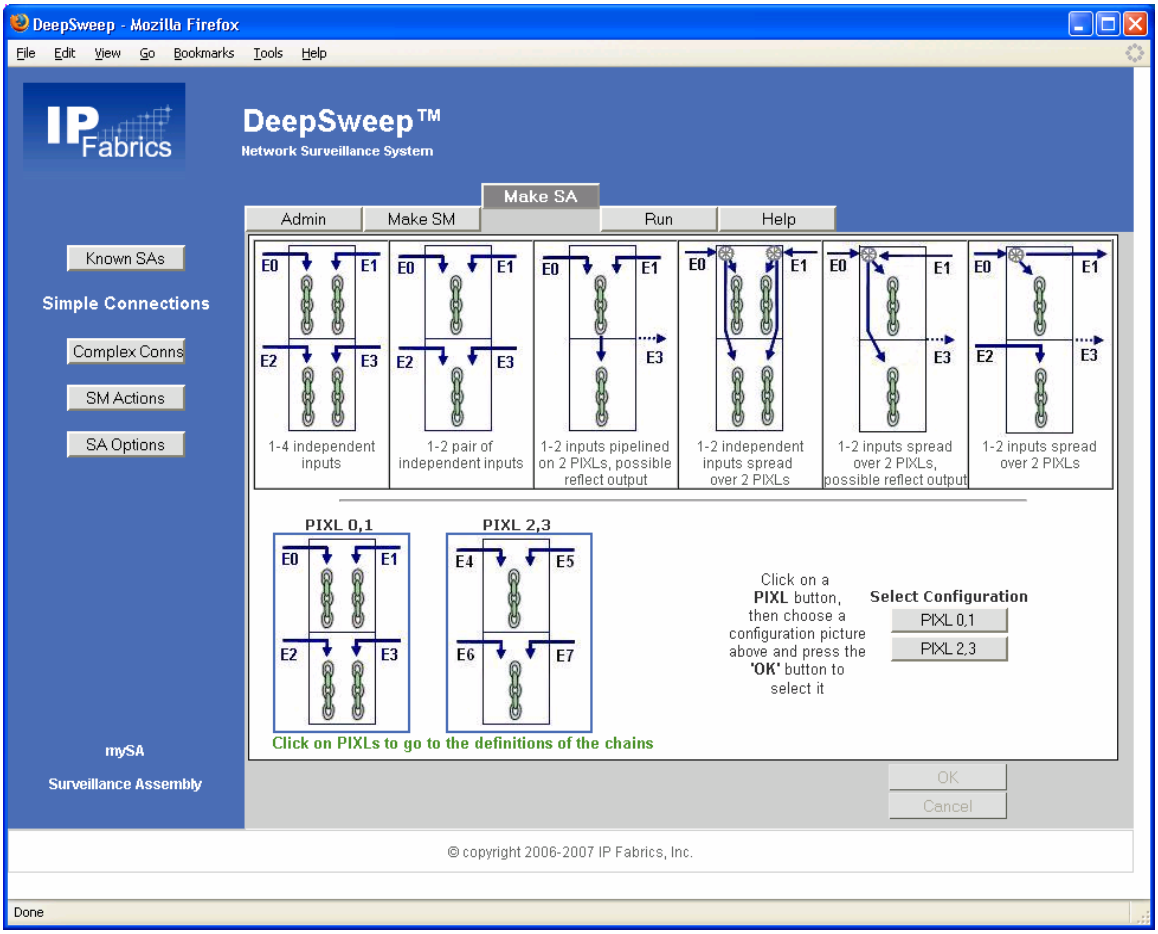


Figure 16. Two PIXL Surveillance Assembly Connections Configuration

The text beneath each icon describes the basic idea for each choice. The topology logic is also depicted graphically. Each SM chain performs the processing specified by the SM Chains page configuration (described later). Hits are processed according to the **SM Options** page selections and can be "reflected" out an interface and/or sent to a subsequent element in the chain or a chain on another PIXL.

If you have an 8-port DeepSweep then there are additional topologies supported. These are shown in Figure 17. As before, to select a configuration topology click on the PIXL 0-3 button, then click the desired topology then click OK.

To configure the chains for each PIXL, first click on the left-hand PIXL pair (bottom of page), complete the SM Chains definition with "OK" and return to the Complex Connections to repeat the process for the second (right-hand) PIXL pair.

 Copyright © IP Fabrics, Inc. 2007

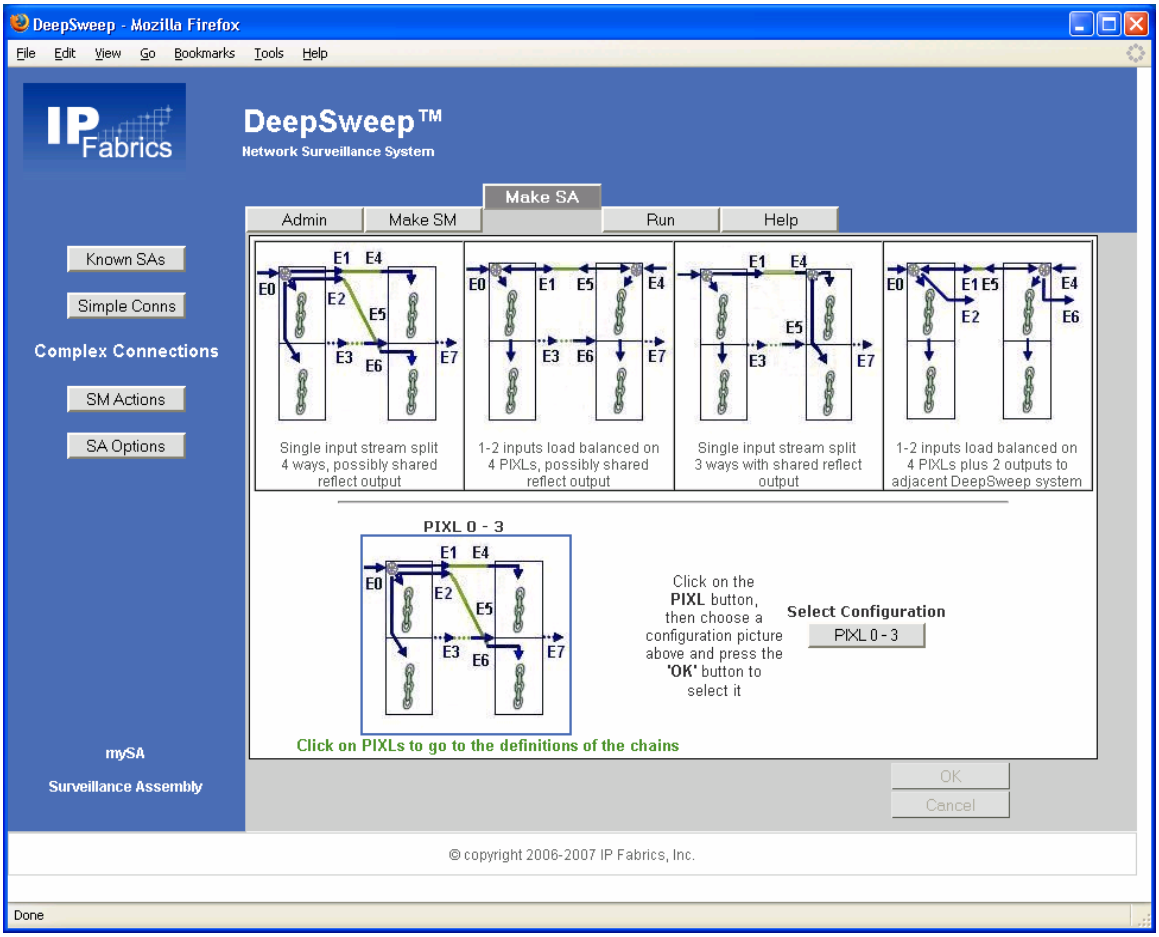

DeepSweep - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
IP Fabrics
DeepSweep™
Network Surveillance System
Make SA
Admin
Make SM
Run
Help
Known SAs
Simple Conns
Complex Connections
SM Actions
SA Options
mySA
Surveillance Assembly
Single input stream split 4 ways, possibly shared reflect output
1-2 inputs load balanced on 4 PIXLs, possibly shared reflect output
Single input stream split 3 ways with shared reflect output
1-2 inputs load balanced on 4 PIXLs plus 2 outputs to adjacent DeepSweep system
PIXL 0 - 3
Click on the PIXL button, then choose a configuration picture above and press the 'OK' button to select it
Select Configuration
PIXL 0 - 3
Click on PIXLs to go to the definitions of the chains
OK
Cancel
© copyright 2006-2007 IP Fabrics, Inc.
Done

Figure 17. Complex Connections configuration page

The green solid lines indicate interconnections you make externally by running an Ethernet cable from one DeepSweep port to another. Note that some are bidirectional. Note that some come from a distributor (wheel). Note that some are dashed lines to indicate they are "reflected" hit packets. . While most applications do not require any complexity at all, the connections pages enable a vast amount of flexibility for the DeepSweep user when needed.

Keep in mind that the **Connections** pages and the SM Chains page must be tightly coordinated. If your connections page causes traffic to flow through a specific SM chain on a PIXL, make sure you configure that chain on the SM Chains page to have the needed SM(s) for proper processing.

4.3.3.3 SM Chains Page

Access to this page is done by clicking on top of the chains to be configured on one of the **Connections** pages (**Simple** or **Complex**). You will only be presented with the number of X and Y chains for the topology icons you selected. If you have two pairs of PIXLs (i.e. an eight-port DeepSweep) then you must click both left and right PIXL pairs to configure all chains.

The previous section focused on interconnecting PIXLs in various ways to provide the processing power needed for the application. We talked about how the **Connections** pages and distribution functions can split traffic across PIXLs. In this section we'll discuss how to use the SM Chains page to create the SM chains on each PIXL for the application.

Figure 18 below highlights the features of the SM chains page. The PIXL-pair being configured is selected back on the **Connections** page by clicking on each of the PIXL pairs in turn. That action is what brings you to the **SM Chain**s page. The figure shows that PIXL 0 and 1 are being displayed.

 Copyright © IP Fabrics, Inc. 2007

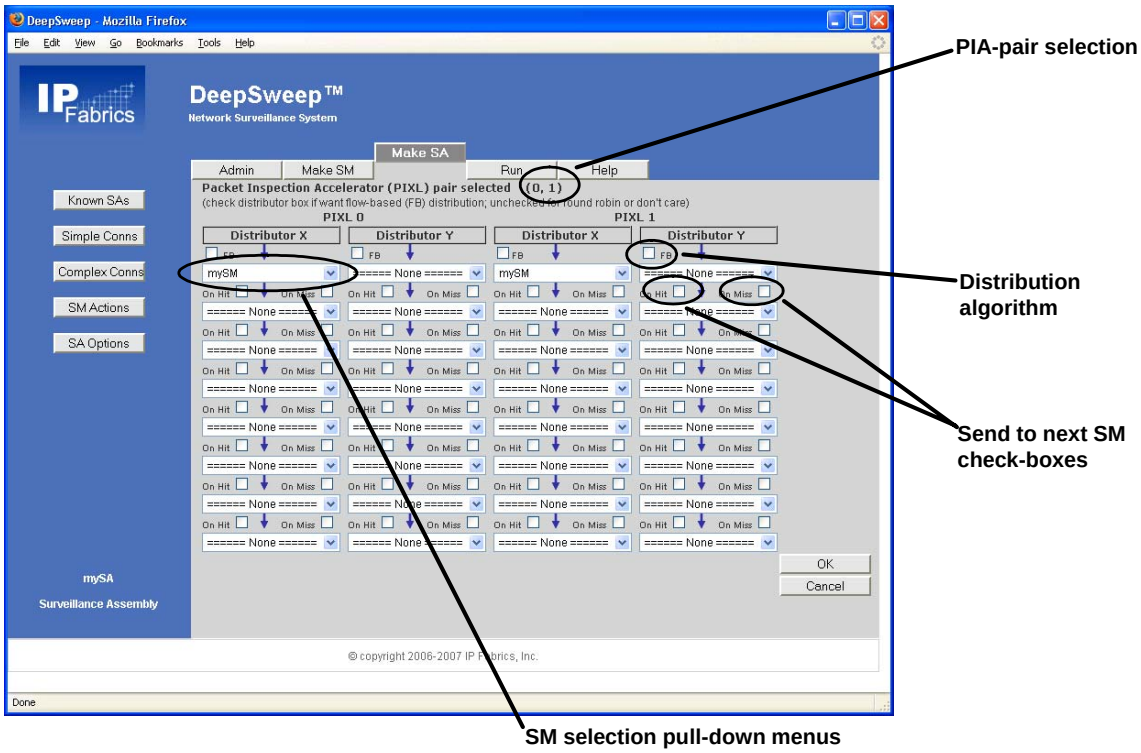


Figure 18. Make SA Tab, SM Chains Page

Each SM chain can contain up to eight SMs. Traffic for each SM is processed sequentially from top to bottom on this page. You'll notice Chain X for PIXL 0 starts at the top with Distributor X, which passes to the SM defined at the top pull-down menu. The check-box labeled "FB" between the Distributor and the first SM in the chain is used to define the distribution algorithm. The "FB" stands for "Flow Based". If the box is checked, the distributor will ensure that packets belonging to the same flow will travel the same distribution path. If not checked, the distributor will simply evenly distribute packets amongst each output path from the distributor. Round robin is faster than flow based distribution, so if the application isn't trying to keep track of flows and simply looking for specific items of interest within a given packet, use the round robin algorithm (i.e. don't check the FB box).

The pull-down lists will display all defined SMs in the DeepSweep. The user can simply select the SM in the list for that position. Note that SMs are created by using the "Make SM" tab described later. For now, just know that you will create and name SMs and those SMs will show up in the pull down menus on this page.

There are two check boxes between each SM pull-down list labeled "On Hit" and "On Miss". These check boxes define when packets will be passed to the next SM in the chain. If "On Hit" is selected, packets matching the hit criteria will be sent along to the next SM. If "On Miss" is selected, packets NOT matching the hit criteria will be sent to the next SM. Both boxes may be checked, so all packets regardless of hit or miss may pass to the next SM.

Note that if there is an SM defined as "NONE" between two valid SMs in a chain, the SM after the "NONE" will never get a packet because the first "NONE" in the chain from top to bottom signals the end of the chain.

Once all SMs are configured, the distribution algorithm is selected, and send-to-next SM check boxes are configured, select "OK" to commit the configuration.

4.3.3.4 SM Actions Page

Once the **SM Chains** page has been configured and committed, selecting the SM Actions button will take you to the **SM Actions** page. This page displays all the SMs used for the surveillance assembly along with a series of check boxes for defining what actions will be taken when hits are found for that SM. The **SM Actions** page is shown in Figure 19.

 Copyright © IP Fabrics, Inc. 2007

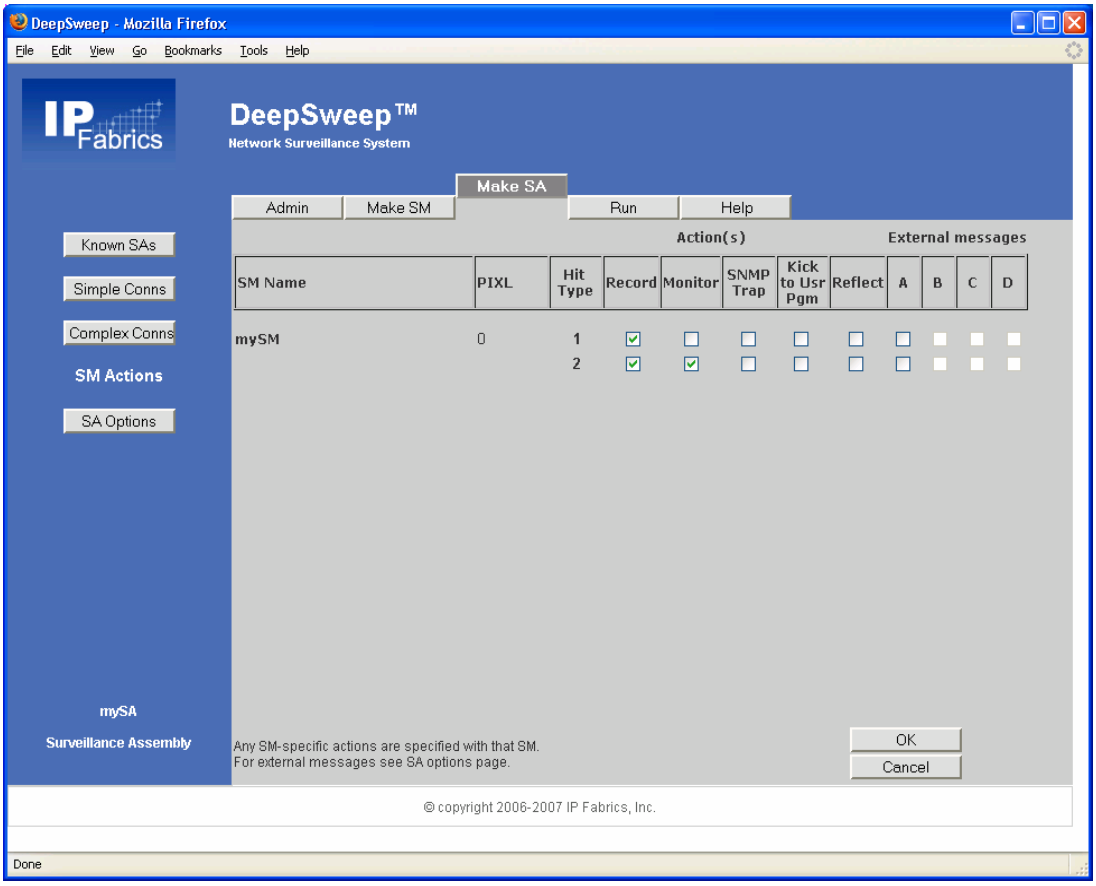


Figure 19. Make SA Tab, SM Actions Page

Looking at this page, there is only one SM defined in the SA – "mySM". This SM shows up on PIXL 0 only. There are two hit types for "mySM". Each hit type can be configured to execute a unique set of actions by selecting the check box(es) for that hit type on the page. In this example, type 1 and type 2 hits will cause DeepSweep to record the packet causing that hit. Also, this example has also selected type 2 hits to appear in the **Monitor** page display. Note that only one set of actions can be configured for an SM name. For instance, if the same SM name shows up in multiple places in the SM chains making up the SA, it will only show up once in this list and the actions configured for that SM name will apply everywhere it shows up in the SA. If you want a different set of actions then create new SM name and set the actions performed for the new SM name on this page.

A surveillance machine can be programmed to send up to four external messages[1]. Format of these external messages can be configured using the SA Options page covered in the next section.

Refer to section 4.3.5 for a description of all the actions an SM can perform.

4.3.3.5 SA Options Page

The **SA Options** page configures the global characteristics of surveillance assembly operation. This page is broken into configuration options for actions, evidentiary record generation, external messaging, network interface characteristics, and user program configuration. The SA Options page is shown in Figure 20.

[1] Currently only 1 external message (A) is supported.

 Copyright © IP Fabrics, Inc. 2007

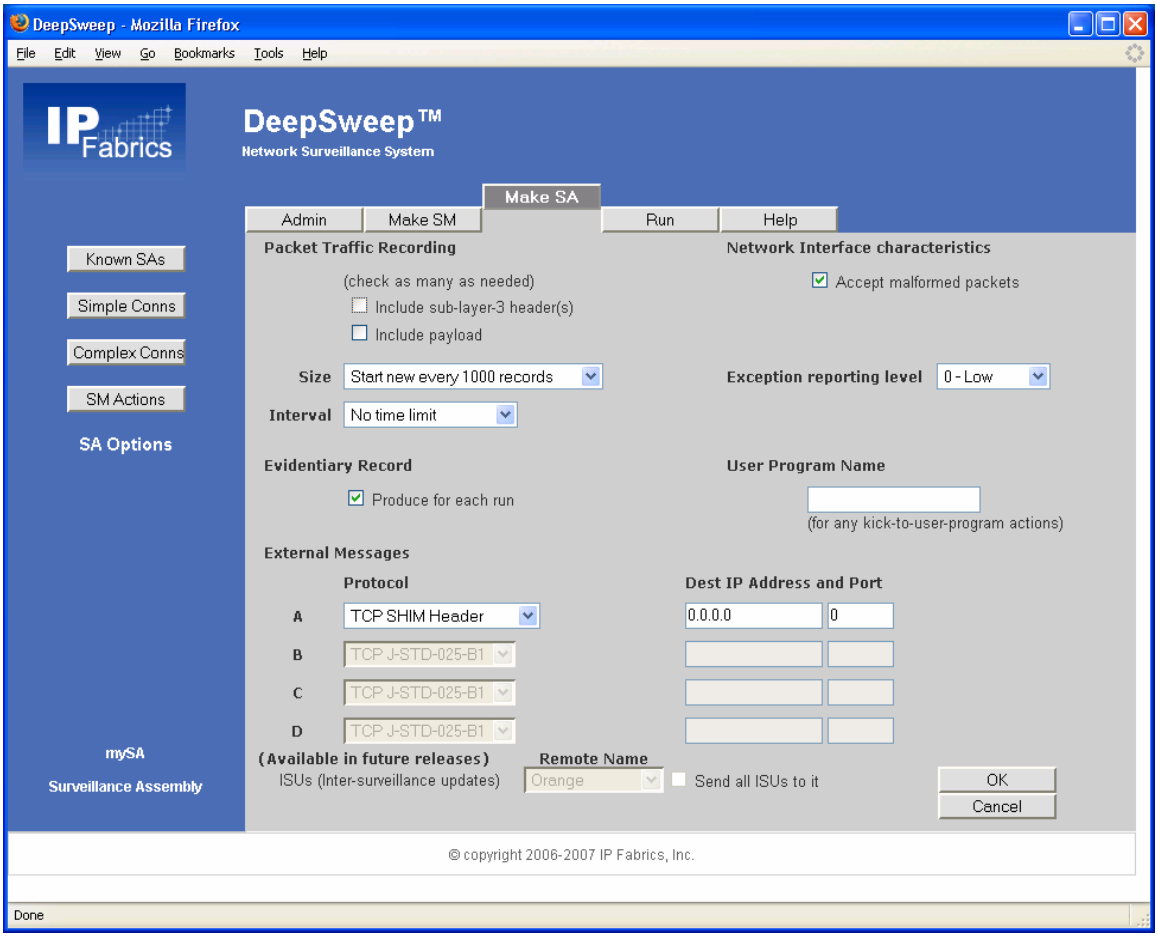


Figure 20. Surveillance Assembly Options Page

The record action for a surveillance assembly records only the layer 3 (IP) and 4 headers of the packet by default. By checking the "include sub-layer 3 header(s)" check box. The record action will write from the beginning of the packet through the layer 4 header in the record file. If the "include payload" box is checked, the record action will also write the contents of the packet after the layer 4 header to the record file.

Checking the "Make evidentiary record" box will cause DeepSweep to generate an evidentiary record with every run of this surveillance assembly. For more information on evidentiary records, see section 4.4.

The external messages section on the page allows the user to configure the format and remote systems that will receive the external messages sent by the SMs. Messages sent currently include part/all of the packet causing the hit and sending the frame to a remote host using TCP or UDP. Like the record action, the external message format can be configured to send just the layer 3 & 4 information, from start of packet through layer 4, and/or include the entire packet payload after layer 4.

The pull-down menu for the DeepSweep names will include all remote DeepSweeps configured through the World View page in the Admin tab, section 4.3.1.2[2].

The user program name for the "hand off 'kick' to user program" action is initialized for the SA on this page. One user program can be initialized for an SA, so all SMs that have "kick to user program" enabled will send the hit to the same user program configured here.

[2] Not available in this release of DeepSweep.

 Copyright © IP Fabrics, Inc. 2007

4.3.4 Surveillance Modules

To this point, we've looked at the overall administration of DeepSweep and toured how to configure a surveillance assembly. In this section, we'll discuss **surveillance modules** (SMs), the processing components that are put on SM chains within a surveillance assembly. Each SM type has its own specific processing that will be described in the specific Surveillance Machine users manual. The information in this section pertains to all SMs.

A surveillance module is an independent building block that performs a specific function/set of functions within a surveillance machine. DeepSweep™ SM types are listed below:

- **Packet Traffic**. This SM detects IP addresses and protocols, stores information about new communicating pairs of IP addresses, and can search for strings, patterns, and regular expressions in the content of a packet.
- **Packet Flow**: This SM can trigger on new connections being made over the network, store state information, and search for strings, regular expressions, or patterns in the traffic payload.
- **Sub_IP**. This SM looks at Ethernet, MPLS, and PPP protocols and finds interesting packets relating to these protocols that live below the IP layer.
- **IAS Controller**. This SM configures case management for the broadband (T1.IAS) CALEA intercept functions.
- **IAS Content**. This SM defines content capture parameters for the broadband (T1.IAS) CALEA intercept functions.
- **VoIP Controller**. This SMconfigures case management for the VoIP (T1.678) CALEA intercept functions.
- **VoIP Content**. This SM defines content capture parameters for VoIP (T1.678) CALEA intercept functions.
- **User Connection**. This SM tracks specific user connections. It supports both static and dynamic methods for user identification.

When selecting the Make SM tab, you're taken to the Known SMs page. Here you'll see a list of SM names that have been defined on the DeepSweep™ with buttons that allow you to create, delete, or edit SM names.

 Copyright © IP Fabrics, Inc. 2007

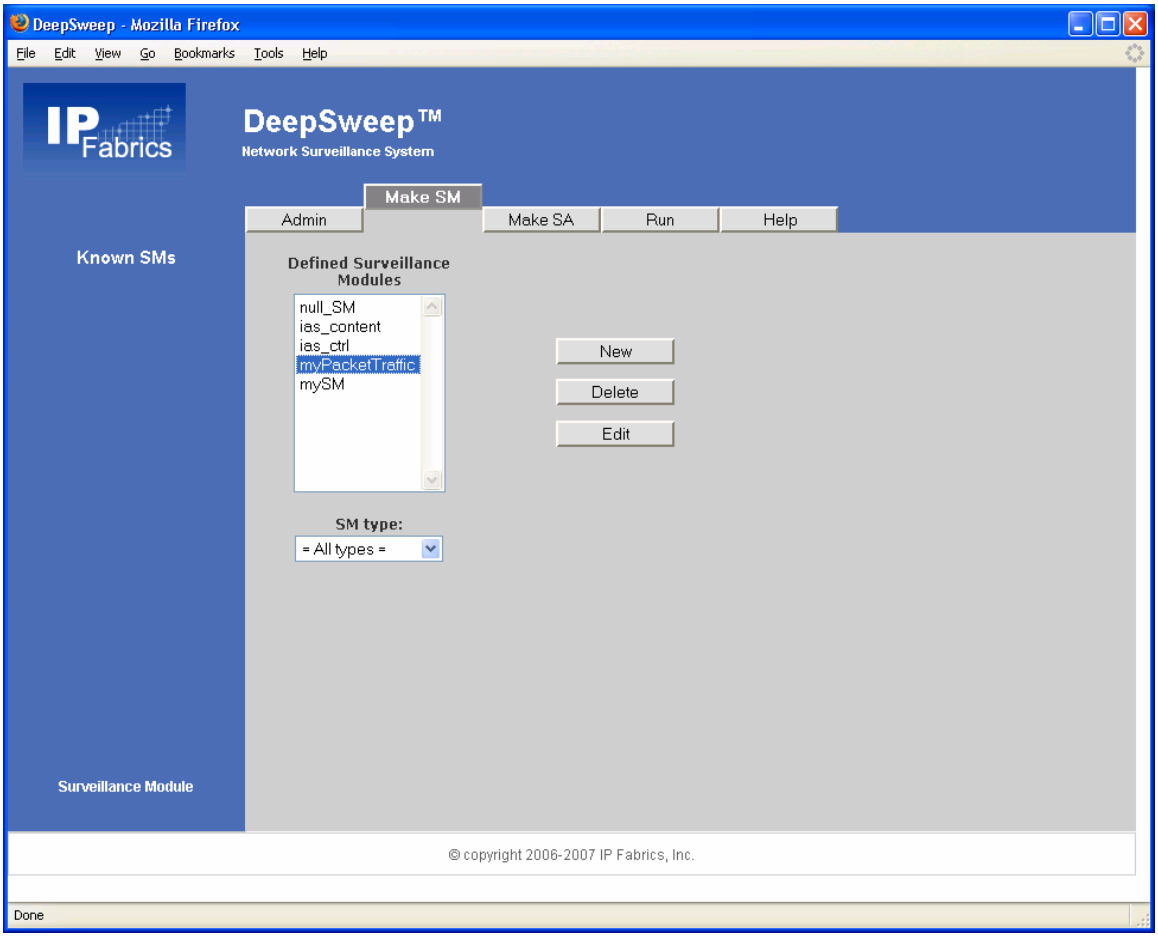
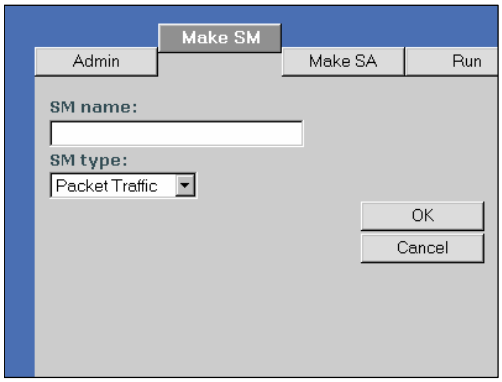


Figure 21. Make Surveillance Module (SM) Page



Clicking the New button will cause a text box and drop-down menu to appear. You can type in the name of the SM and what type it is from here. SM names can be any alphanumeric name including periods and underscores. Once the name and its type are configured, clicking the "OK" button commits this SM name and returns to the Make SM main page. Once there, you should see the newly created SM in the list.

To edit an SM, select it from the list and hit the "Edit" button. Once Edit is selected, the main page for that specific SM type is displayed. The configuration pages for each SM type are described below.

To delete an SM, simply select the SM name from the list and click the "Delete" button.

For more detail on specific SM types, refer to the user's manual for that SM type.

 Copyright © IP Fabrics, Inc. 2007

4.3.5 Surveillance Module Actions

All SM types provide the same set of actions when hits occur. Actions on hits are configured through the SM Actions page of the Make SM tab shown in section 4.3.3.4. Each of these actions is listed below with a description of what these actions do and which configuration pages relate to those actions.

4.3.5.1 SNMP Trap Action

The SNMP trap action causes an SNMP trap to be sent by the SM when a packet is identified as a hit. At the **Admin** tab, **World View** page, there are SNMP options that also need to be set up. There is an SNMP enable check box and a text box for the SNMP trap recipient. In order for the trap action to work, this check box needs to be checked to enable SNMP and a valid IP address for the SNMP trap recipient programmed in the text box.

The SNMP trap enable/disable and trap recipient address is set globally for all surveillance assemblies on the DeepSweep™.

4.3.5.2 Record Action

The record action causes part or all of the packet to be recorded in a record file. The record file will be placed in the ENS user-accessible area via secure FTP login. The name of the file is in the form:

[*Surveillance Assembly name*]_[*timestamp*].pcap.

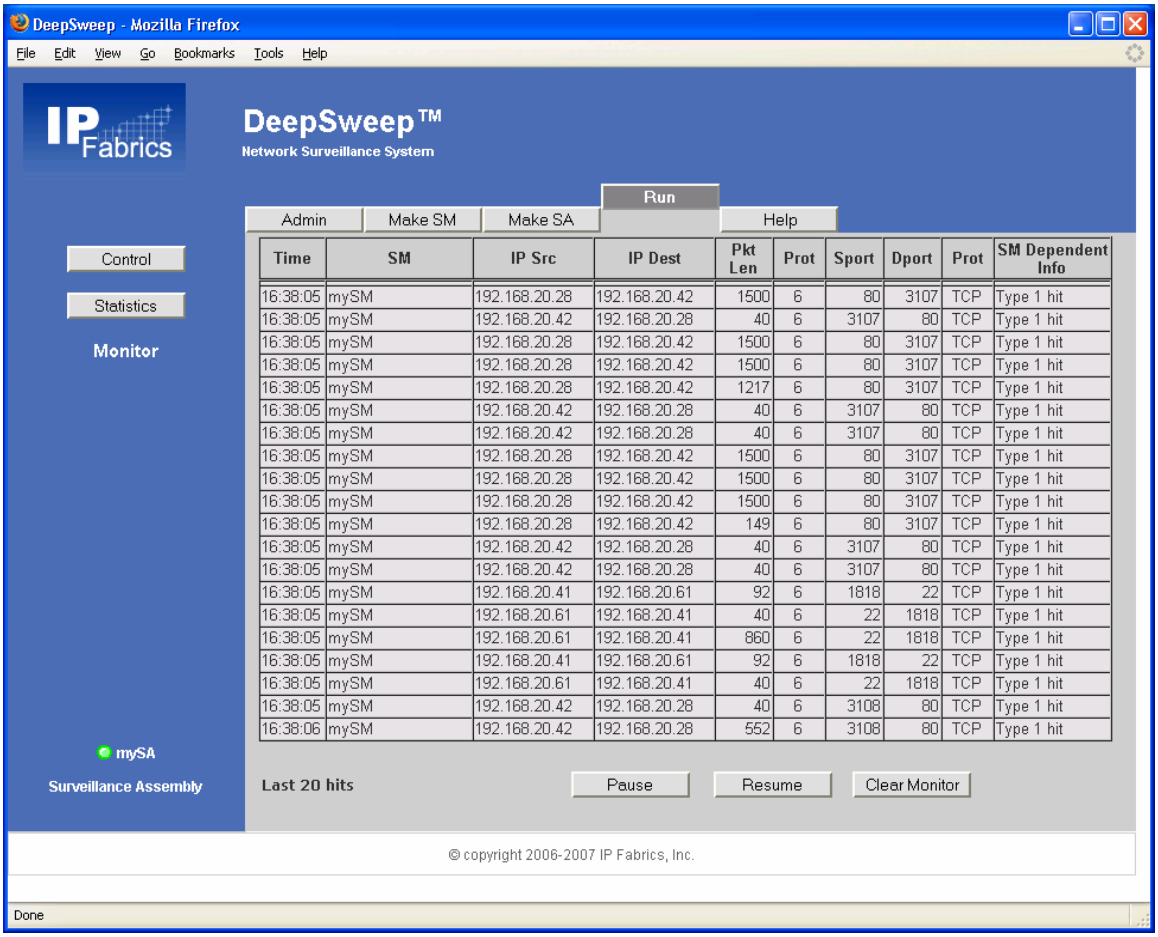
This file is in standard PCAP file format and is readable using Ethereal/Wireshark and other programs that understand PCAP. If you do use one of these programs then you will get the best results by checking the "Include sub-layer-3 header(s)" on the **SA Options** page under the **Make SA** tab.

Configuration options for the record file are accessible at the **Make SA** tab, **SA Options** page. On that page, you'll see check boxes that allow you to set how much of the packet is to be recorded. This characteristic can be set differently for each surveillance assembly.

4.3.5.3 Monitor Action

The monitor action causes packet information to be sent to the monitor page of the Run tab.

 Copyright © IP Fabrics, Inc. 2007



Time	SM	IP Src	IP Dest	Pkt Len	Prot	Sport	Dport	Prot	SM Dependent Info
16:38:05	mySM	192.168.20.28	192.168.20.42	1500	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.42	192.168.20.28	40	6	3107	80	TCP	Type 1 hit
16:38:05	mySM	192.168.20.28	192.168.20.42	1500	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.28	192.168.20.42	1500	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.28	192.168.20.42	1217	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.42	192.168.20.28	40	6	3107	80	TCP	Type 1 hit
16:38:05	mySM	192.168.20.42	192.168.20.28	40	6	3107	80	TCP	Type 1 hit
16:38:05	mySM	192.168.20.28	192.168.20.42	1500	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.28	192.168.20.42	1500	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.28	192.168.20.42	1500	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.28	192.168.20.42	149	6	80	3107	TCP	Type 1 hit
16:38:05	mySM	192.168.20.42	192.168.20.28	40	6	3107	80	TCP	Type 1 hit
16:38:05	mySM	192.168.20.42	192.168.20.28	40	6	3107	80	TCP	Type 1 hit
16:38:05	mySM	192.168.20.41	192.168.20.61	92	6	1818	22	TCP	Type 1 hit
16:38:05	mySM	192.168.20.61	192.168.20.41	40	6	22	1818	TCP	Type 1 hit
16:38:05	mySM	192.168.20.61	192.168.20.41	860	6	22	1818	TCP	Type 1 hit
16:38:05	mySM	192.168.20.41	192.168.20.61	92	6	1818	22	TCP	Type 1 hit
16:38:05	mySM	192.168.20.61	192.168.20.41	40	6	22	1818	TCP	Type 1 hit
16:38:05	mySM	192.168.20.42	192.168.20.28	40	6	3108	80	TCP	Type 1 hit
16:38:06	mySM	192.168.20.42	192.168.20.28	552	6	3108	80	TCP	Type 1 hit

Figure 22. DeepSweep Monitor Page

The monitor page is shown above. You'll notice the monitor page prints out in real time, the timestamp and packet information. You can allow your screen cursor to hover over an entry to see any information that is too long to fit in the display box.

4.3.5.4 External Message Action

The external messages action causes hits to be sent over a socket to a remote host for further processing. On the **Make SA** tab, **SA Options** page, the Destination IP address and port number as well as the method for sending for up to four messages is set in the pull-down menu and two text boxes on that page.

4.3.5.5 Hand off "Kick" to user program action

DeepSweep™ allows user programs to be loaded onto the system and interface with the running surveillance assembly through the "kick to user program" action. The DeepSweep™ file system contains a template for a user program that can be used and enhanced for specific applications. The name of the user program to execute is configurable from the **Make SA** tab, **SA Options** page.

4.3.5.6 Real-Time Statistics page

Real-time statistics are also being kept when the SA is running. This page can be accessed from the **Run** tab by selecting the Statistics button.

The statistics boxes at the top of the page are running counters as packets come in on the Ethernet interfaces. The boxes grouped by chains are the statistics for each SM in the SA. Each SM keeps up to four statistics. All SMs keep a total packets statistic in the lower right box. All SMs also keep type 1 hit statistics in the upper left box. For SMs that define

 Copyright © IP Fabrics, Inc. 2007

type 2 statistics, this counter shows up in the upper right hand corner. For SMs keeping type 3 hit statistics, this counter is in the lower left corner of the box.

You can discover additional information about the stats on the right by allowing your cursor to "hover" over an entry. Note that the stats refresh rates is selectable with a pull-down menu.

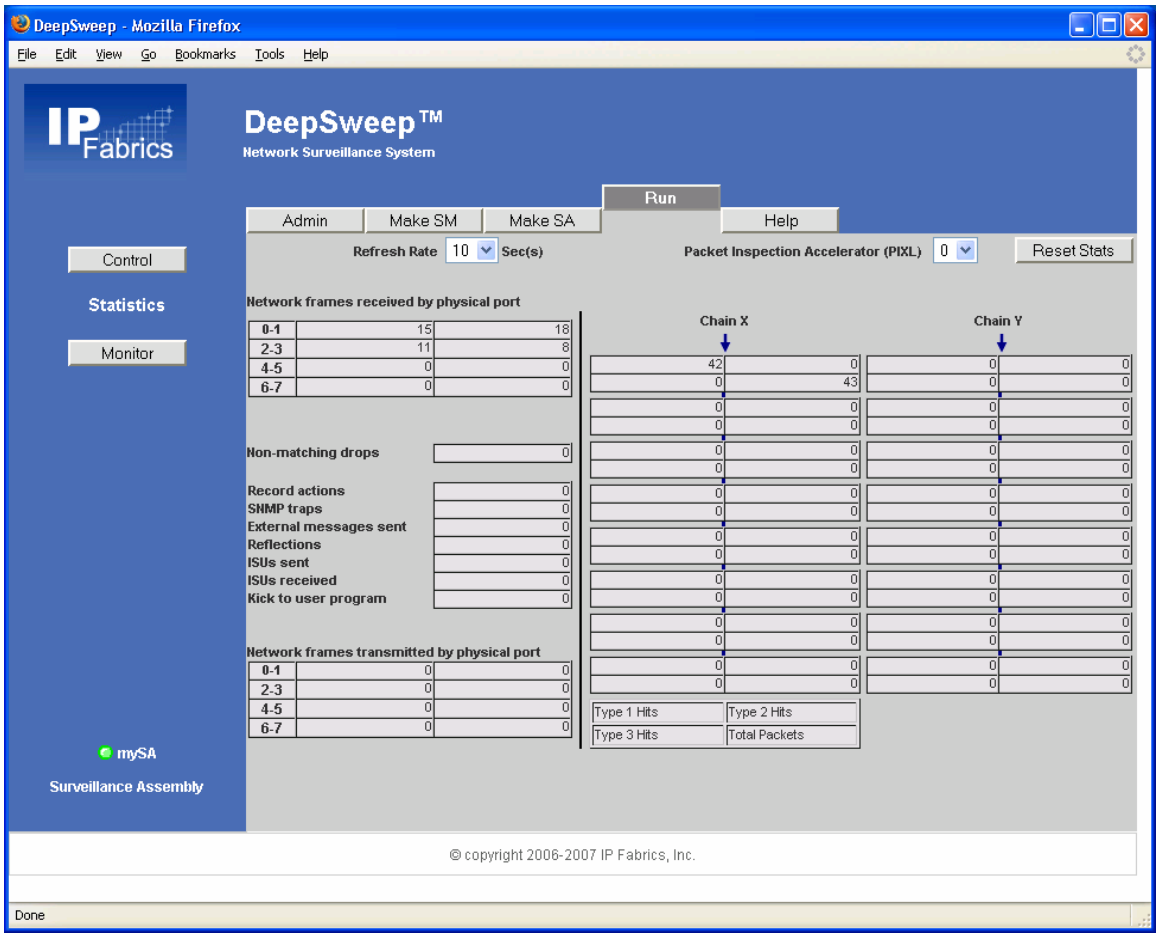


Figure 23. Real-Time Statistics Page

4.3.6 Databases

Databases are used by the DeepSweep™ system when a packet needs to matched against a large dataset. The packet fields of interest to match can either be a packet header or the packet content. Two types of databases are used depending on the type of these fields. They are described below.

4.3.6.1 Classify Database

Classify databases provide an effective method of specifying a large set of packet header field values that need to be matched against an incoming packet. The match criteria for each field can be specified as an operation performed with the stored value in the database and appropriate field in the packet.

Section 6 covers the format of Classify databases in detail. Each classification database input file is a simple ASCII text file which needs to be copied into the in DeepSweep™ system using the secure FTP mechanism. Specifying the

 Copyright © IP Fabrics, Inc. 2007

database's filename in the appropriate field on the Pre-Filter page of the SM will ensure that the SM includes that Classify database in its processing.

4.3.6.2 Patterns Database

Patterns databases provide a convenient method of specifying a large set of patterns (content strings) that need to be matched against an incoming packet's header and/or content fields. The DeepSweep™ uses an optimized algorithm to match multiple patterns simultaneously against an incoming packet's contents. These matches can also be associated with optional tags which can be used to further qualify a match.

Section 7 covers the format of Patterns databases in detail. Each Patterns database input file is a simple ASCII text file which needs to be copied into the in DeepSweep™ system using the secure FTP mechanism. Specifying the database's filename in the appropriate field on the Filter page of the SM will ensure that the SM includes that Patterns database in its processing.

4.3.6.3 Updating the Databases for an SA During Operation

Dynamic database updates can be performed while DeepSweep is running from the **Run** tab, **Control** page. Simply load the updated database into the DeepSweep user area, then select that database name in the pull-down menu. Once the correct database has been selected, click the "Update" button to initiate the dynamic update of the new database. You'll be asked if you're sure you want to do this – answer "ok" and the system will complete the update.

4.4 Evidentiary Records

As described in 4.3.3.5, DeepSweep™ may be configured to produce an evidentiary record for each Surveillance Assembly. The evidentiary record is intended to document the exact configuration of the Surveillance Assembly, its component Surveillance Modules, and any results collected by the same, for use in court or other legal proceedings.

Each evidentiary record describes one run of one particular Surveillance Assembly. Multiple runs of the same Surveillance Assembly result in multiple evidentiary records.

4.4.1 Contents

Each evidentiary record contains:

- A friendly (text) description of the Surveillance Assembly and its component Surveillance Modules. This information is distilled from the various SA and SM pages.
- A pair of timestamps describing when the Surveillance Assembly was started, and when it was halted.
- Copies of all Classify and Patterns databases provided by the user.
- Summary statistics collected by the Surveillance Assembly at runtime
- Version information about the DeepSweep™ itself.

4.4.2 Enabling Evidentiary Records

To enable evidentiary records for a given Surveillance Assembly, select the corresponding check box on the SA Options page (see figure Figure 20). To disable evidentiary records for a given Surveillance Assembly, leave this check box blank. This setting will automatically take effect the next time this Surveillance Assembly is launched.

4.4.3 Location of Evidentiary Records

Each evidentiary record contains dynamic information collected by the Surveillance Assembly at run-time, and therefore the evidentiary record is not available until the Surveillance Assembly has been stopped.

When the current Surveillance Assembly is halted, the resulting evidentiary record is placed in the FTP directory where it may be retrieved via FTP/SSH or other secure protocol.

The resulting evidentiary record consists of two files:

- Atext file containing the surveillance and system data listed above. This file is named: ***`evidentiary_record_<surveillance assembly name>_<timestamp>.txt`***.

 Copyright © IP Fabrics, Inc. 2007

- A file containing the SHA1 hash of the text file. This is a simple text file and contains only the SHA1 hash value computed over the tar file. This file is named: ***evidentiary_record_<surveillance assembly name>_<timestamp>.sha1***.

The hash value is provided to prevent or detect tampering with the contents of the tar file. DeepSweep™ computes this hash value immediately after finalizing the tar file, before making either file available for download.

.

 Copyright © IP Fabrics, Inc. 2007

5 Creating User Defined Programs for DeepSweep™

Advanced DeepSweep™ users may wish to run custom surveillance programs on the DeepSweep to further process packet hits. This capability is supported through the "kick to user program" action described briefly in section 4.3.5.5. The action allows the DeepSweep™ user to configure a user program and UDP port number where the DeepSweep™ will send hits.

Requirements for creating user programs for DeepSweep™:

- Must know Linux application programming and C++ (although creation of a program in another language that can open a socket will also suffice).
- Must have direct access to the DeepSweep™ Linux file system through a console in order to write, compile, and debug the user program.

A template user program is found in the DeepSweep™ file system at **`/ens/src/user_pgm_template`**. This template allows the programmer access to packet input from the running surveillance assembly and perform special processing for the surveillance activity.

5.1 Building the User Program

The template user program provides a Makefile and source files for the starting point of the user program. Only one of the provided C++ class source files need be modified – all the rest should be able to be left alone for proper operation. The **`UserPgm.hpp`** file contains a constructor and **`process()`** method where the custom code can be inserted.

The constructor code should initialize whatever is needed for the user program during execution. The user program template **`process()`** method will be called whenever a hit is received from the surveillance assembly. The parameters for the **`process()`** method are a packet buffer pointer and size parameters.

Once the user program is created, the provided Makefile can be used to build the program. The Makefile has two additional directives:

- **`make clean`** – will delete the intermediate and executable files. So, the next time make is run, everything will rebuild.
- **`make purge`** – will delete just the executable file. The intermediate files are left. So, making after a purge won't rebuild source that has been unmodified since the last build.

Once successfully built, place the user program in the /ens/bin directory where it will be automatically run when the surveillance assembly using it starts.

5.2 Available SA Services

The user program has the ability to use two surveillance assembly resources – the DeepSweep™ log and record files.

The user program can write to the record file by using the following method:

```
void writeToRecordFile(Socket* s, u_int8_t *buffer, u_int32_t size);
```

This method will write size bytes of the buffer parameter to the record file.

Likewise, the user program can write to the log file by using the following method:

```
void writeToLogFile(Socket* s, u_int8_t *buffer, u_int32_t size);
```

This method will write size bytes of the buffer parameter to the DeepSweep™ log file.

5.3 User Program Configure, Load, and Run

Once the user program has been successfully generated, follow the steps below to link it to the surveillance assembly:

1. Copy the user program executable into the **`/ens/bin`** directory.
2. Add the "kick to user program" action to an SM on the Make SA tab, SA Actions page.
3. On the Make SA tab, SA Options page, add the file name of the user program put into /ens/bin from step 1.

 Copyright © IP Fabrics, Inc. 2007

Once these steps are complete, go to the **Run** tab, **Control** page. Select the surveillance assembly that uses your user program and click the **Run** button. Your user program should now show up in the Linux process table. You can verify this by typing "**`ps -ef`**" at the Linux console and looking for the name of your user program in the process table.

If your program doesn't appear to be running, look in the **`/var/ens/vmd.pid`** file. The **`printf()`** statements from your user program should show up in this log file. If there were errors starting your user program, they will also show up in this file.

 Copyright © IP Fabrics, Inc. 2007

6 Creating Classify Databases

Classification databases can be set up to be used by SM's such as "Packet Traffic" through the Pre-Filter page.

A Classification database can be thought of being composed of columns containing values that the incoming packet is going to be classified against. Each column is a particular field in the packet (will be explained in detail later) and is of a known size. Each value within the column is coupled with an operator (some operators have optional masks) that will be applied to the packet field before matching it to the value in the column. The value within the column is treated as though it has been already "masked" if the operator has a mask is specified with it.

A Classification database hit is obtained when each value in a given row is an "operational" match to the appropriate packet field.

Classification database filenames by convention usually end with the ".cls" extension.

A template of the input file is as follows:

```
 <CLASSIFYDB NAME="Classification_database_name">
col_specification_line
data row
.
.
.
data row
</CLASSIFYDB>
<DATA>. . .</DATA>
```

The first line in the input file is expected to have the following format:

```
<CLASSIFYDB NAME="Classification_database_name">
```

The string within the quotes gives the name of the Classification database. The name is of the database is required and an error is signaled if it is omitted.

The next line or the "column specification" (col_spec) line gives the size attributes of the various columns of the database. The col_spec line has the following format.

```
size …[up to 7 more of "size"]
```

SIZE has the following values QUAD, WORD, HALF and BYTE and specifies the width of the column to be 128 bits, 32bits 16 bits or 8 bits respectively. Table 2 has a listing of possible comparators. The col_spec line can contain one or more "size" but their total number is limited to 8. Therefore a Classification database can have a maximum of 8 columns.

For Example,
```
QUAD WORD HALF BYTE...
```

The individual "size" specifications are delimited by white spaces.

The two lines described above have to be the first two lines of the input file otherwise an error will result when database is processed.

The column data values are specified in the subsequent lines or data row lines. A limitation in the current implementation is the total number of bytes that are available for data values in a data row. This value is between 48 and 50 bytes depending on the number of columns. Each data row line is terminated by a "new line" character or each unique data row starts on a new line in the file.

The data row line has the following format

 Copyright © IP Fabrics, Inc. 2007

```
[operator] data_value…[up to 7 more of "[comparator] data_value"
                                                              pairs]
```

The accepted data values are listed in the table below.

Format	Comments
d[d…]	One of more digits 0..9
0xhh[hh…]	0x followed by one or more pairs of digits 0..F
num.num.num.num	A 32-bit value where num is 0..255
Hn:hn:hn:hn:hn:hn:hn:hn	A 128-bit value where hn is 0..FFFF. IPv6 double-colon notation for zero compression is also permitted (e.g., FF02::2)
'c[c..]'	One or more characters within the single quotes, each of which represented an 8-bit encoding. Use **\n** for new line character. Use **\'** to specify a single quote character and **** to specify a backslash character
FuF	The 32-bit value 0xFFFFFFFF

Table 1. Accepted Value Formats

Some operators have an optional mask for a few operations. A list of the operators is specified in Table 2.

For Example,

```
EQ 0x10     NE 192.168.0.1    EQ/8 'AB'   GT 1234
```

White space characters are delimiters for data values and operators. The total number of data value and operator pairs cannot exceed the number of columns as specified by the col_spec line. This number is limited to a maximum value of 8 as mentioned before.

Any rows with values that are less than the total number of columns will have the missing value's comparators set to the "XX" or "don't care" operator with value itself set to 0 as per the column size.

The last line of the input file for the classification data values is always in the format below.

```
</CLASSIFYDB>
```

The table below has the complete listing of the Classification database operators.

 Copyright © IP Fabrics, Inc. 2007

Operation	Classification Database Operator	Usage Example
Empty (never matches)	**ZZ**	**ZZ** 0
Always match (don't care, ignore value)	**XX**	**XX** 0
Equals	**EQ**	**EQ** 0x1234
Does not equal	**NE**	**NE** 'ne'
Less than	**LT**	**LT** 1234
Less than or equal	**LE**	**LE** 'le'
Greater than	**GT**	**GT** 1234
Greater than or equal	**GE**	**GE** 'ge'
Equals, after masking from left n = 1..127 for QUAD, 1..31 for WORD, 1..15 for HALF and 1..7 for BYTE	**EQ/n**	**EQ/16** 10.1.0.0
Does not equal, after masking from left n = 1..127 for QUAD, 1..31 for WORD, 1..15 for HALF and 1..7 for BYTE	**NE/n**	**NE/16** 0xCOA80000
Equals, after masking from right n = 1..127 for QUAD, 1..31 for WORD, 1..15 for HALF and 1..7 for BYTE	**EQ//n**	**EQ//16** 0x00000A01
Does not equal, after masking from right n = 1..127 for QUAD, 1..31 for WORD, 1..15 for HALF and 1..7 for BYTE	**NE//n**	**NE//16** 0.0.40.1
Equals, after direct byte mask m is a 8 bit mask	**EQbm**	**EQb0xe0** 0x06
Does not equal, after direct byte mask m is a 8 bit mask	**NEbm**	**Neb224** 6

Table 2. Classification Operators Listing

The last line in the input file has the following format.

```
<DATA>PKT_FLD1,...PKT_FLDn</DATA> …[n <= 8]
```

The number of packet fields specified need to be equal to the number of columns in the Classification database. Each packet field is separated by a comma.

The table below has a complete listing of the packet fields that can be specified.

Packet Field Name	Definition
IP_VERSION	
IP_HDRLEN	IPv4 only
IP_TOS_TC_DS	8-bit value in first word of IP header. If IPv4, bits 8-15. If IPv6, bits 4-11.
IP_TOSPREC	Bits 0-2 of IP_TOS_TC_DS (meaningful in IPv4 only)
IP_TOSTOS	Bits 3-6 of IP_TOS_TC_DS (per RFC 1349, meaningful in IPv4 only)
IP_DSCP	Bits 0-5 of IP_TOS_TC_DS (per RFC 2474)
IP_DSECN	Bits 6-7 of IP_TOS_TC_DS (per RFC 3168)
IP_PACKETLEN	IPv4 only
IP_IDENTIFIER	IPv4 only
IP_DF	IPv4 only
IP_MF	IPv4 only
IP_FRAGOFFSET	IPv4 only
IP_TTL	IPv4 only
IP_HDRCSUM	IPv4 only

 Copyright © IP Fabrics, Inc. 2007

Packet Field Name	Definition
IP_FLOWLABEL	IPv6 only
IP_PAYLOADLEN	IPv6 only
IP_HOPLIMIT	IPv6 only
IP_PROT	IPv4 and IPv6. In IPv6, this is not in a fixed place. When used (read), It is identical to IP_NEXTHDR unless IP_NEXTHDR has one of the values 0, 43, 44, or 60, in which case IP_PROT is the next-header field of the first extension whose value is other than 0, 43, 44, 60. When stored, it is treated identical to IP_NEXTHDR.
IP_NEXTHDR	IPv6 only. Always the 6th byte of the IP header.
IP_SOURCE	Source IP address
IP_DEST	Destination IP address
L4_SPORT	Source port in the IP payload assuming it is a layer 4 protocol containing this field
L4_DPORT	Destination port in the IP payload assuming it is a layer 4 protocol containing this field
ICMP_TYPE	
ICMP_CODE	
UDP_LENGTH	
UDP_CSUM	
TCP_SEQNUM	
TCP_ACKNUM	
TCP_DATAOFFSET	
TCP_FLAGS	Bits 8-15 in 4th word of TCP header
TCP_CWR	Bit 0 in flags
TCP_ECE	Bit 1 in flags
TCP_URG	Bit 2 in flags
TCP_ACK	Bit 3 in flags
TCP_ACKONLY	Means ACK without FIN or SYN Cannot be destination
TCP_PSH	Bit 4 in flags
TCP_RST	Bit 5 in flags
TCP_SYN	Bit 6 in flags
TCP_SYNONLY	Means SYN without ACK or FIN Cannot be destination
TCP_SYNACK	Means SYN and ACK Cannot be destination
TCP_FIN	Bit 7 in flags
TCP_WINDOW	
TCP_CSUM	
TCP_URGPTR	
PS_IP	Boolean specifying that the packet is an IP packet.
PS_TCPUDP	Boolean specifying that the packet is either TCP or UDP protocol. Shorthand for testing if IP_PROT is equal to TCP or UDP.
PS_FRAGMENT	Boolean specifying that the packet is a fragment. For an IPv4 packet this indicates that either IP_FRAGOFFSET is nonzero or that IP_MF is set. For an IPv6 packet this indicates that a fragment extension header is present.
PS_NOORFIRSTFRAG	Boolean specifying that the packet is not a fragment or is the first fragment. For an IPv4 packet this indicates that IP_FRAGOFFSET is zero. For an IPv6 packet this indicates that either there is no fragment extension header, or there is one and its fragment offset value is zero.
PS_EXTENDEDHDR	Boolean specifying that the packet has extended headers. For an IPv4 packet, this indicates that IP_HDRLEN > 5. For an IPv6 packet, this indicates that IP_NEXTHDR has one of the values: 0, 43, 44, 50, 51, or 60.

 Copyright © IP Fabrics, Inc. 2007

Packet Field Name	Definition
PS_IPDATASIZE	Value specifying the number of bytes of data in the packet after the outermost IP with options and extensions. For IPv4 this is IP_PACKETLEN minus 4 times IP_HDRLEN. For IPv6 this is the value IP_PAYLOADLEN minus the size of all extension headers present.
PS_IPDATAOFFSET	Value specifying the byte offset of the first data byte after the IP header(s) (measured from the start of the IP header).
PS_CONTENTSIZE	Value currently defined only if a UDP or TCP packet – specifies the content length in bytes not included the TCP or UDP header. This is identical to PS_IPDATASIZE minus the length of the TCP or UDP header.
PS_CONTENTOFFSET	Value defining the CONTENT base – the byte offset (relative to the start of the IP header) of the first byte beyond the TCP, UDP, or ICMP header, or of the first byte beyond the outermost IP header if IP_PROT is not one of these.

Table 3. Packet Fields Listing

So a complete Classification database input file with 4 columns is shown below.

```
<CLASSIFYDB NAME="simple">
QUAD        WORD              HALF        BYTE
EQ 0x10     NE 192.168.0.1    EQ/8  'A0'  GT 1
LE  245     EQ 0x12345678     NE//8 0x18  LT 'F'
LE  245     GT 0x12345678     EQ//8 0x18  LE 'F'
</CLASSIFYDB>
<DATA>IP_SOURCE, IP_DEST, L4_SPORT, L4_DPORT </DATA>
```

 Copyright © IP Fabrics, Inc. 2007

7 Creating Patterns Databases

Patterns databases can be set up to be used by SM's such as "Packet Traffic","Packet Traffic" through the Filter pages.

Patterns database provide a convenient method to specify a large number of strings or packets that needs to matched against a packet's payload.

A Patterns database hit is obtained when any pattern within the database has a match in the incoming packet's payload.

Patterns database filenames by convention end with the ".pat" extension.

The following XML DTD describes the Patterns database input file.

```
<!DOCTYPE PATTERNDB [
      <!ELEMENT PATTERNDB (PATTERN)+>
      <!ATTLIST PATTERNDB NAME (#PCDATA)?>
      <!ELEMENT PATTERN (#PCDATA)>
      <!ATTLIST PATTERN CASE NMTOKEN "sensitive"
                        TAG (#PCDATA)?
                        TAGMASK (#PCDATA)?
                        ID (#PCDATA)?
      >
]>
```

This leaves an input file format that looks like the example below.

```
<PATTERNDB NAME="MY_PAT_DB">
  <PATTERN>ipfabrics</PATTERN>
  <PATTERN>Spiderman &amp; Superman</PATTERN>
  <PATTERN CASE="insensitive">This is whaT we are Looking for</PATTERN>
  <PATTERN>performance ??????? most</PATTERN>
  <PATTERN>>|CAFEFACE|</PATTERN>
</PATTERNDB>
```

The string within the quotes in the first line gives the name of the Patterns database. The name is of the database is required and an error is signaled if it is omitted.

The pattern string is by default a character string. Enclosing part or all of the pattern string in vertical bars ("|") will cause that section of the string to be treated as hexadecimal input. Inserting a '?' into the string inserts a wildcard at that position. It is an error to use all 256 possible byte values in a pattern that includes a wild card. In order to insert a question mark or vertical bar into the actual search string, it must be escaped with a backslash ('\').

Attributes to the patterns are:

CASE	By default, patterns are case "sensitive" but can be set to case insensitive setting this attribute to "insensitive".
TAG	The 32 bit tag value to include with this pattern, normally unset. Numbers starting with "0x" are hexadecimal, with "0" are octal and decimal otherwise.
TAGMASK	Four mask bits which indicate which bytes in the tag are actually in use. If no tag has been specified, this defaults to 0000, 1111 if a tag has been specified. The value is given in binary.
ID	The ID value to return when this pattern is matched. By default the compiler will number the patterns in ascending order starting at 1. If a pattern is given a low enough ID, it is possible for the patterns processor to assign other patterns the same ID.

When a TAG is specified an additional line is required in the database input file to specify as what the TAG(s) correspond to.

 Copyright © IP Fabrics, Inc. 2007

```
<TAG_QUAL>PKT_FLD1,...PKT_FLDn</TAG_QUAL> …[1..n = 32 bits]
```

Since each TAG is 32 bits the total number of bits of the packet fields should equal 32 bits. If more then 1 packet fields are specified then each individual one is separated by a comma. The listing of packet fields is given in Table 3.

A complete Patterns database input file is shown below.

```
<PATTERNDB NAME="MY_PAT_DB">
      <PATTERN>1234</PATTERN>
      <PATTERN>CAFE MOCHA</PATTERN>
      <PATTERN TAG="0xBEAD" TAGMASK="0011">ipfabrics</PATTERN>
      <PATTERN TAG="0xCAFEBEEF" TAGMASK="1100">Dude! I found
 it</PATTERN>
      <PATTERN>where is it\?</PATTERN>
      <PATTERN CASE="insensitive">pplvm</PATTERN>
      <PATTERN>greenbrier parkway</PATTERN>
      <PATTERN>|CAFEBEEF|</PATTERN>
      <PATTERN>the quick brown fox jumps over a lazy dog</PATTERN>
      <PATTERN>ThE QuIck BROWN foX jumPs OveR a LazY DOg</PATTERN>
      <PATTERN>performance ??????? most</PATTERN>
      <PATTERN>tireless striving </PATTERN>
      <PATTERN>stretches its arms </PATTERN>
      <PATTERN>towards perfection </PATTERN>
      <PATTERN TAG="0xACEDFACE" TAGMASK="1111">Found IT </PATTERN>
      <PATTERN>1234 98765</PATTERN>
      <PATTERN>Hello World</PATTERN>
      <PATTERN>IP Fabrics, Inc.</PATTERN>
      <PATTERN>Double Espresso</PATTERN>
      <PATTERN CASE="insensitive">This is whaT we are Looking for</PATTERN>
      <PATTERN>Spiderman &amp;amp; Superman</PATTERN>
      <PATTERN>show me the m@ney, the ca$h</PATTERN>
      <PATTERN>\|looking for a dreadnought guitar\|</PATTERN>
      <PATTERN>&lt; Sean George Roger Timothy Pierce Craig &gt;</PATTERN>
      <PATTERN>thisisalongpatterntotestlongpatternsitshouldnothaveanyproblembuti
ncasethereisaproblemweneedtofixthisbecausefixingproblemsiseasyonceyouknowthatthe
reisaproblemtobefixed</PATTERN>
      <TAG_QUAL>L4_SPORT, L4_DPORT</TAG_QUAL>
</PATTERNDB>
```

 Copyright © IP Fabrics, Inc. 2007

8 Accounts and Ports Information

The table below has a list of type of accounts, their usernames and default passwords in the DeepSweep™ system.

Account Type	Username	Password	Comments
DeepSweep Admin Account	admin	ipfabrics	The default admin account that system comes preconfigured with.
DeepSweep User Account	(Assigned by admin)	ipfabrics	The default password is always the same. The user can change it once s/he is logged in.
FTP Account to the DeepSweep System	ens_administrator	ipfabrics	The file transfer account to use to transfer database and other files to the DeepSweep System. Supports FTP, SFTP and SCP. **NOTE**: The password should be changed by owner upon installation.
DeepSweep Linux Account	root	ipfabrics	The root account for the Linux OS. **NOTE**: The password should be changed by owner upon installation.
DeepSweep Linux Account	ipfabrics	ipfabrics	Used internally during execution and also for PPL development for custom applications. **NOTE**: The password should be changed by owner upon installation.

The table below has a list of Ethernet ports and the IP address they are set to.

Host	Physical port	O/S view of port	IP address	Mask	Comments
DeepSweep	NIC 1 on rear	'eth0'			Enabled for DHCP initially. Can be used for browser.
DeepSweep	NIC 2 on rear	'eth1'	192.168.43.50	255.255.252.0	Static IP. Can be used by browser.
DeepSweep	(internal only)	'eth2'	192.168.100.1	255.255.255.0	ONLY USED FOR internal SWITCH. Static IP; used to boot NPU's. Not cabled – connected directly to switch card.

 Copyright © IP Fabrics, Inc. 2007

Appendix A –'iptables' reference firewall file

The following is a valid referencefirewall configuration for DeepSweep system.
The file is located in the directory: `/etc/sysconfig/iptables`

```
# Generated by iptables-save v1.2.11 on Tue Oct  9 16:14:21 2007
*filter
:INPUT DROP [14650:1913513]
:FORWARD DROP [0:0]
:OUTPUT DROP [7:280]
:DYNAMIC_INPUT - [0:0]
:USER_INPUT - [0:0]
:USER_OUTPUT - [0:0]
-A INPUT -s 127.0.0.1 -j ACCEPT
-A INPUT -i pxd+ -j ACCEPT
-A INPUT -p tcp -m tcp --dport 9536 -j ACCEPT
-A INPUT -p udp -m udp --dport 9536 -j ACCEPT
-A INPUT -p tcp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -j DYNAMIC_INPUT
-A INPUT -j USER_INPUT
-A OUTPUT -d 127.0.0.1 -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -j USER_OUTPUT
-A DYNAMIC_INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A DYNAMIC_INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A DYNAMIC_INPUT -j RETURN
-A USER_INPUT -p tcp -m tcp --dport 161 -j ACCEPT
-A USER_INPUT -p udp -m udp --sport 123 --dport 123 -j ACCEPT
-A USER_INPUT -p icmp -m limit --limit 10/sec -j ACCEPT
-A USER_INPUT -j RETURN
-A USER_OUTPUT -p udp -m udp --sport 123 --dport 123 -j ACCEPT
-A USER_OUTPUT -p icmp -m limit --limit 10/sec -j ACCEPT
-A USER_OUTPUT -j RETURN
COMMIT
# Completed on Tue Oct  9 16:14:21 2007
```

 Copyright © IP Fabrics, Inc. 2007

Appendix B –'ntp.conf'reference file

The following is a valid reference NTP configuration file for DeepSweep system.
The file is located in the directory: `/etc/ntp.conf`

```
#
# ntp.conf
#
# NTP configuration file for the ENS host.  Lifted verbatim from the
# default RedHat NTP configuration file, with a few extra tweaks.
# Should be installed as /etc/ntp.conf
#

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.

restrict default nomodify notrap noquery

# Permit all access over the loopback interface.  This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1

# -- CLIENT NETWORK -------
# Permit systems on this network to synchronize with this
# time service.  Do not permit those systems to modify the
# configuration of this service.  Also, do not use those
# systems as peers for synchronization.
# restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# IPF -- Allow the XScales to synchronize their clocks to this host
restrict 192.168.100.0 mask 255.255.255.0 nomodify notrap

# --- OUR TIMESERVERS -----
# IPF -- Assume ENS deployment within the continental US
server 0.us.pool.ntp.org
server 1.us.pool.ntp.org
server 2.us.pool.ntp.org

# --- NTP MULTICASTCLIENT ---
#multicastclient                        # listen on default 224.0.1.1
# restrict 224.0.1.1 mask 255.255.255.255 nomodify notrap
# restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# --- GENERAL CONFIGURATION ---
#
# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available. The
# default stratum is usually 3, but in this case we elect to use stratum
# 0. Since the server line does not have the prefer keyword, this driver
# is never used for synchronization, unless no other other
# synchronization source is available. In case the local host is
# controlled by some external source, such as an external oscillator or
# another protocol, the prefer keyword would cause the local host to
```

 Copyright © IP Fabrics, Inc. 2007

```
# disregard all other synchronization sources, unless the kernel
# modifications are in use and declare an unsynchronized condition.
#
server  127.127.1.0     # local clock
fudge   127.127.1.0 stratum 10

#
# Drift file.  Put this in a directory which the daemon can write to.
# No symbolic links allowed, either, since the daemon updates the file
# by creating a temporary in the same directory and then rename()'ing
# it to the file.
#
driftfile /var/lib/ntp/drift
broadcastdelay  0.008

#
# Keys file.  If you want to diddle your server at run time, make a
# keys file (mode 600 for sure) and define the key number to be
# used for making requests.
#
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will. Note also that
# ntpd is started with a -A flag, disabling authentication, that
# will have to be removed as well.
#
#IPF keys               /etc/ntp/keys
```

 Copyright © IP Fabrics, Inc. 2007